kaspersky

Kaspersky SD-WAN

© 2026 AO Kaspersky Lab

Índice

Ajuda do Kaspersky SD-WAN

Sobre o Kaspersky SD-WAN

- Kit de distribuição
- Requisitos de hardware e software
- Garantia de segurança

Novidades

Arquitetura da solução

Implementar o Kaspersky SD-WAN

- Redundância de componentes da solução
- Configurar o balanceamento de carga entre instâncias do orquestrador
- Sobre o arquivo de instalação
- Sobre os modos de ação assistido, autônomo e parcialmente assistido
- Preparar o dispositivo do administrador
- Gerenciar senhas
  - Gerar senhas manualmente
  - Alterar senhas
- Preparar o arquivo de configuração
- Substituir os gráficos da interface da Web do orquestrador
- Substituir um nó do controlador com falha
- Fazer upgrade do Kaspersky SD-WAN
- Remover o Kaspersky SD-WAN

Fazer login e logout da interface da Web do orquestrador

Licenciamento do Kaspersky SD-WAN

- Sobre o Contrato de Licença do Usuário Final
- Sobre a coleta de dados

Interface do usuário da solução

- Configurar e redefinir a página padrão
- Alternar entre os modos claro e escuro da interface da Web do orquestrador
- Alterar o idioma da interface da Web do orquestrador
- Gerenciar tabelas de componentes da solução

Navegar até a API do orquestrador

Gerenciar a infraestrutura do Kaspersky SD-WAN

- Gerenciar domínios
  - Criar um domínio
  - Editar um domínio
  - Excluir um domínio
- Gerenciar data centers
  - Adicionar um data center
  - Editar um data center
  - Migrar um data center para um domínio diferente
  - Excluir um data center

- Gerenciar sub-redes de gerenciamento
  - Criar uma sub-rede de gerenciamento
  - Editar uma sub-rede de gerenciamento
  - Excluir uma sub-rede de gerenciamento
- Gerenciar controladores
  - Editar um controlador
  - Reprovisionar um controlador
  - Restaurar as configurações do controlador
  - Ativar ou desativar o modo de manutenção em um controlador
  - Excluir um controlador
  - Gerenciar as propriedades do controlador
    - Descrição das propriedades editáveis do controlador
    - Editar uma propriedade do controlador
    - Excluir valores planejados das propriedades do controlador
    - Redefinir propriedades do controlador para os valores padrão
  - Visualizar informações sobre nós do controlador
- Gerenciar um VIM
  - Configurar um VIM implementado em um data center
  - Configurar um VIM implementado em um dispositivo uCPE
  - Editar um VIM implementado em um data center
  - Visualizar recursos de computação sendo usados por um VIM
  - Excluir um VIM
- Gerenciar usuários e suas permissões de acesso
  - Gerenciar permissões de acesso
    - Criar permissões de acesso
    - Editar permissões de acesso
    - Clonar permissões de acesso
    - Remover uma permissão de acesso
  - Gerenciar conexões LDAP
    - Criar uma conexão LDAP
    - Editar uma conexão LDAP
    - Alterar a senha de uma conexão LDAP
    - Excluir uma conexão LDAP
  - Gerenciar usuários
    - Criar um usuário
    - Ativar ou bloquear um usuário
    - Editar um usuário
    - Alterar a senha de um usuário local
    - Autenticação de dois fatores repetida de um usuário
    - Excluir uma conta de usuário
  - Gerenciar grupos de usuários LDAP
    - Criar um grupo de usuários LDAP
    - Editar um grupo de usuários LDAP
    - Excluir um grupo de usuários LDAP
  - Ativar ou desativar a autenticação de dois fatores para todos os usuários
  - Gerenciar solicitações de confirmação
  - Gerenciar sessões de usuário

- Multilocação
  - Cenário: implementar uma instância SD-WAN para um locatário
  - Gerenciar locatários
    - Criar um locatário
    - Atribuir um usuário a um locatário
    - Atribuir um grupo de usuários LDAP a um locatário
    - Atribuir recursos de computação a um locatário
    - Atribuir componentes do serviço de rede a um locatário
    - Atribuir um VIM a um locatário
    - Fazer login no portal de autoatendimento do locatário
    - Editar um locatário
    - Excluir um locatário
  - Gerenciar modelos de instância SD-WAN
    - Criar um modelo de instância SD-WAN
    - Definir o modelo de instância SD-WAN padrão
    - Selecionar o número de nós do controlador para uma instância SD-WAN
    - Adicionar um locatário a um modelo de instância SD-WAN
    - Remover um locatário de um modelo de instância SD-WAN
    - Excluir um modelo de instância SD-WAN
  - Gerenciar instâncias SD-WAN
    - Configurar os nós do controlador de uma instância SD-WAN
    - Visualizar o uso de uma instância SD-WAN
    - Visualizar a topologia de uma instância SD-WAN
    - Adicionar um locatário a uma instância SD-WAN
    - Remover um locatário de uma instância SD-WAN
    - Excluir uma instância SD-WAN
  - Gerenciar pools de instâncias SD-WAN
    - Criar um pool de instâncias SD-WAN
    - Adicionar uma instância SD-WAN a um pool de instâncias SD-WAN
    - Remover uma instância SD-WAN de um pool de instâncias SD-WAN
    - Excluir um pool de instâncias SD-WAN
- Gerenciar dispositivos CPE
  - Sobre a interação do dispositivo CPE com o orquestrador
  - Sobre a interação do dispositivo CPE com o controlador
  - Credenciais padrão dos dispositivos CPE KESR
  - Verificação de integridade
  - Registrar dispositivos CPE
    - Cenário: registro automático de um dispositivo CPE usando a tecnologia Zero Touch Provisioning.
    - Cenário: implementar um dispositivo vCPE na plataforma de virtualização VMware e registrá-lo usando a tecnologia Zero Touch Provisioning
    - Cenário: registrar novamente um dispositivo CPE
    - Retomar o registro do dispositivo CPE em caso de erro
  - Gerenciar modelos de CPE
    - Criar um modelo de CPE
    - Importar um modelo de CPE
    - Clonar um modelo de CPE
    - Exportar configurações de conexão do orquestrador e do controlador e interfaces SD-WAN de um modelo de CPE

- Exportar interfaces de rede de um modelo de CPE
- Visualizar o uso de um modelo de CPE
- Excluir um modelo de CPE

Gerenciar dispositivos CPE

- Adicionar dispositivos CPE
- Importação em massa de dispositivos CPE de um arquivo CSV
- Gerar uma URL com configurações básicas do dispositivo CPE
- Registrar um dispositivo CPE manualmente
- Cancelar o registro de um dispositivo CPE
- Especificar o endereço de um dispositivo CPE
- Ativar e desativar um dispositivo CPE
- Reiniciar um dispositivo CPE
- Desligar um dispositivo CPE
- Conectar-se ao console do dispositivo CPE
- Visualizar a senha de um dispositivo CPE
- Exportar configurações de conexão do orquestrador e do controlador e interfaces SD-WAN de um dispositivo CPE
- Exportar interfaces de rede de um dispositivo CPE
- Alterar o DPID de um dispositivo CPE
- Editar as configurações do dispositivo CPE
- Excluir dispositivos CPE

Autenticação de dois fatores de um dispositivo CPE

Gerenciar certificados

- Carregar um certificado usando a interface da Web do orquestrador
- Instalar certificados manualmente em dispositivos CPE
- Cenário: instalar certificados em um dispositivo CPE com firmware versão 23.07
- Exportar um certificado
- Excluir certificados

Gerenciar diretórios APN

- Criar um diretório APN

Exibir e redefinir sessões em dispositivos CPE

Excluir e desativar dispositivos CPE automaticamente

Agrupar dispositivos CPE usando tags

- Atribuir uma tag a dispositivos CPE
- Remover uma tag de dispositivos CPE

Configurar logs em dispositivos CPE

Gerenciar modems

Atualizar o firmware

- Atualizar o firmware em um dispositivo CPE manualmente
- Carregar firmwares para a interface da Web do orquestrador
- Agendar atualizações de firmware em dispositivos CPE selecionados
- Agendar atualizações de firmware em dispositivos CPE com tags específicas
- Restaurar o firmware de um dispositivo CPE KESR-M1
- Restaurar o firmware de um dispositivo CPE KESR-M2-5
- Correspondência de modelos de dispositivo CPE com versões de firmware
- Excluir um firmware

Configuração adicional de dispositivos CPE usando scripts
Adicionar um script a dispositivos CPE
Executar manualmente um script em dispositivos CPE
Agendar scripts em dispositivos CPE
Editar um script em dispositivos CPE
Excluir um script em dispositivos CPE
Gerenciar configurações de DNS em dispositivos CPE
Ativar o DNS em interfaces de rede
Gerenciar o encaminhamento condicional de DNS
Criar regras de encaminhamento condicional
Editar regras de encaminhamento condicional
Excluir regras de encaminhamento condicional
Configurar a conexão de um dispositivo CPE com orquestrador e controlador
Gerenciar as configurações de conexão do dispositivo CPE usando o console do sistema
Gerenciar interfaces de rede
Criar interfaces de rede
Criar uma interface de rede com atribuição automática de um endereço IP via DHCP
Criar uma interface de rede com um endereço IPv4 estático
Criar uma interface de rede com um endereço IPv6 estático
Criar uma interface de rede para estabelecer conexão com uma rede LTE
Criar uma interface de rede para estabelecer conexão com um servidor PPPoE
Criar uma interface de rede sem um endereço IP
Editar uma interface de rede
Desativar ou ativar uma interface de rede
Cancelar a aplicação de configurações da interface de rede em um dispositivo CPE
Excluir uma interface de rede
Proteção contra Spoofing de IP usando uRPF
Gerenciar interfaces SD-WAN
Sobre o envio de informações sobre interfaces SD-WAN do tipo WAN para o controlador
Fragmentação de pacotes
Filas de tráfego em interfaces SD-WAN
Criar uma interface SD-WAN do tipo WAN
Editar uma interface SD-WAN
Desativar ou ativar uma interface SD-WAN
Excluir uma interface SD-WAN do tipo WAN
Gerenciar interfaces de serviço
Criar uma interface de serviço
Criar uma interface ACL
Visualizar o uso de uma interface de serviço e uma interface ACL
Excluir uma interface de serviço ou uma interface ACL
Gerenciar grupos de portas OpenFlow
Criar um grupo de portas OpenFlow
Editar um grupo de portas OpenFlow
Excluir um grupo de portas OpenFlow

Configurar uma UNI para conectar dispositivos CPE a serviços de rede
Gerenciar modelos de UNI
Criar um modelo de UNI
Excluir um modelo de UNI
Gerenciar UNIs
Criar uma UNI
Visualizar a utilização da UNI
Editar uma UNI
Excluir uma UNI
Adicionar uma rota estática
Tabela de correspondência de distâncias administrativas e protocolos de roteamento
Filtrar rotas e pacotes de tráfego
Gerenciar listas de controle de acesso (ACLs)
Criar uma lista de controle de acesso
Editar uma lista de controle de acesso
Excluir uma lista de controle de acesso
Gerenciar listas de prefixos
Criar uma lista de prefixos
Editar uma lista de prefixos
Excluir uma lista de prefixos
Gerenciar listas de comunidades
Criar uma lista de comunidades
Editar uma lista de comunidades
Excluir uma lista de comunidades
Gerenciar mapas de roteamento
Criar um mapa de roteamento
Editar um mapa de roteamento
Excluir um mapa de roteamento
Roteamento baseado em política (PBR)
Gerenciar regras de roteamento de IP
Criar uma regra de IP
Editar uma regra de IP
Excluir uma regra de IP
Troca de rotas por BGP
Configurações básicas de BGP
Gerenciar pares BGP
Criar um par BGP
Editar um par BGP
Excluir um par BGP
Gerenciar grupos de pares BGP
Criar um grupo de pares BGP
Editar um grupo de pares BGP
Excluir um grupo de pares BGP
Configurar vazamento de rota inter-VRF

- Troca de rotas por OSPF
  - Configurações básicas do OSPF
  - Gerenciar áreas OSPF
    - Criar uma área OSPF
    - Editar uma área OSPF
    - Excluir uma área OSPF
  - Gerenciar interfaces OSPF
    - Criar uma interface OSPF
    - Editar uma interface OSPF
    - Excluir uma interface OSPF
- Usar o BFD para detectar falhas de roteamento
  - Ativar ou desativar o protocolo BFD
  - Criar um par BFD
  - Editar um par BFD
  - Excluir um par BFD
- Garantir a alta disponibilidade com o VRRP
  - Ativar ou desativar o protocolo VRRP
  - Gerenciar instâncias VRRP
    - Criar uma instância VRRP
    - Editar uma instância VRRP
    - Excluir uma instância VRRP
  - Gerenciar grupos de instâncias VRRP
    - Criar um grupo de instâncias VRRP
    - Editar um grupo de instâncias VRRP
    - Excluir um grupo de instâncias VRRP
- Transmissão de tráfego multicast usando os protocolos PIM e IGMP
  - Configurações básicas de PIM
  - Gerenciar interfaces multicast
    - Criar uma interface multicast
    - Editar uma interface multicast
    - Excluir uma interface multicast
- Gerenciar tabelas de roteamento e encaminhamento virtual (VRF)
  - Especificar configurações de kernel relacionadas a tabelas de roteamento virtual
  - Criar uma tabela de roteamento e encaminhamento virtual
  - Modificar a tabela de roteamento e encaminhamento virtual
  - Excluir uma tabela de roteamento e encaminhamento virtual
- Monitorar informações de pacotes de tráfego usando o protocolo NetFlow
  - Gerenciar modelos de NetFlow
    - Criar um modelo de NetFlow
    - Selecionar um modelo de NetFlow atribuído
    - Importar um modelo de NetFlow
    - Clonar um modelo de NetFlow
    - Visualizar o uso de um modelo de NetFlow
    - Excluir um modelo de NetFlow
  - Configurações básicas de NetFlow
  - Alterar o modelo de NetFlow de um dispositivo CPE

- Diagnosticar um dispositivo CPE
  - Solicitar informações de diagnóstico
  - Usar o modo de depuração para protocolos de roteamento dinâmico em dispositivos CPE
  - Especificar servidores NTP em dispositivos CPE
  - Ativar o modo interativo
  - Executar o utilitário ping
  - Executar o utilitário traceroute
  - Executar o utilitário tcpdump
  - Executar o utilitário iperf
  - Executar o utilitário sweep
  - Executar o utilitário OpenFlow dump
  - Redefinir sessões de BGP/OSPF
  - Gerenciar relatórios
    - Baixar um relatório
    - Excluir um relatório
- Executar tarefas em dispositivos CPE
  - Criar uma tarefa
  - Executar uma tarefa manualmente
  - Excluir uma tarefa
- Verificações em dispositivos CPE
  - Verificação de integridade
    - Execução manual de uma verificação de integridade
    - Configuração da verificação de integridade agendada
  - Autoteste do firewall
    - Execução manual de um autoteste do firewall
    - Configuração de autoteste de firewall agendado
  - Bloquear tráfego se o autoteste ou a verificação de integridade falhar

Auditoria de eventos de segurança
- Configurar o registro de eventos de segurança para auditoria
- Lista de eventos de segurança que podem ser registrados no orquestrador e nos dispositivos CPE

Intervalos de endereços IP e sub-redes para dispositivos CPE
- Gerenciar intervalos de endereços IP
  - Criar um intervalo de endereços IP
  - Editar um intervalo de endereços IP
  - Visualizar o uso de um intervalo de endereços IP
  - Excluir intervalos de endereços IP
- Gerenciar intervalos de sub-redes
  - Criar um intervalo de sub-redes
  - Editar um intervalo de sub-redes
  - Visualizar o uso de um intervalo de sub-redes
  - Excluir intervalos de sub-redes

Gerenciar o firewall
- Gerenciar zonas de firewall
  - Criar uma zona de firewall
  - Clonar uma zona comum de firewall
  - Visualizar o uso de uma zona comum de firewall

- Editar uma zona de firewall
- Excluir uma zona de firewall

Gerenciar modelos de firewall
- Criar um modelo de firewall
- Selecionar um modelo de firewall atribuído
- Importar um modelo de firewall
- Clonar um modelo de firewall
- Visualizar o uso de um modelo de firewall
- Excluir um modelo de firewall

Configurações básicas de firewall

Configurar a marcação de DPI

Gerenciar regras de firewall
- Criar uma regra de firewall
- Configurar a ordem das regras de firewall
- Ativar ou desativar uma regra de firewall
- Editar uma regra de firewall
- Excluir uma regra de firewall

Gerenciar regras avançadas de firewall
- Critérios de correspondência adicionais para regras avançadas
  - Pacote fragmentado
  - Corresponder por marca
  - TOS
  - Corresponder por string
  - Corresponder por recente
  - Flags TCP inválidas
  - Limite da taxa
  - Código para dispositivos móveis
  - Correspondência por comandos de protocolo da camada de aplicativo
- Criar uma regra avançada
- Ativar e desativar regras avançadas
- Editar uma regra avançada
- Excluir uma regra avançada
- Cenário: ocultar um dispositivo CPE no caminho de tráfego usando regras avançadas de firewall

Gerenciar conjuntos de IPs
- Criar um conjunto de IPs
- Desativar ou ativar um conjunto de IPs
- Editar um conjunto de IPs
- Excluir um conjunto de IPs

Gerenciar regras de DNAT
- Criar uma regra de DNAT
- Configurar a ordem das regras de DNAT
- Desativar ou ativar uma regra de DNAT
- Editar uma regra de DNAT
- Excluir uma regra de DNAT

Gerenciar regras de SNAT
- Criar uma regra de SNAT
- Configurar a ordem das regras de SNAT

Desativar ou ativar uma regra de SNAT
Editar uma regra de SNAT
Excluir uma regra de SNAT
Gerenciar o encaminhamento
Criar um encaminhamento
Excluir um encaminhamento
Alterar o modelo de firewall de um dispositivo CPE
Integração com ferramentas externas de segurança da informação
Gerenciar serviços de rede e virtualização de funções de rede
Gerenciar modelos de serviço de rede
Criar um modelo de serviço de rede
Editar um modelo de serviço de rede
Excluir um modelo de serviço de rede
Gerenciar serviços de rede
Criar um serviço de rede
Editar um serviço de rede
Implementando serviço de rede
Verificar a consistência de um serviço de rede
Reimplementar um serviço de rede
Desativar ou ativar a recuperação automática para um serviço de rede
Visualizar o log do serviço de rede
Excluir um serviço de rede
Cenário: implementar uma função de rede virtual
Cenário: implementar uma função de rede física
Gerenciar pacotes VNF e PNF
Configurar o descritor de VNF
Configurar o descritor de PNF
Proteção de pacotes VNF e PNF contra substituição e modificação
Carregar um pacote de VNF ou PNF para a interface da Web do orquestrador
Especificar uma breve descrição para um serviço de rede compartilhado
Gerenciar funções de rede virtual
Selecionar a variação de uma função de rede virtual
Configurar pontos de conexão externos de uma função de rede virtual
Configurações básicas de uma função de rede virtual
Hospedar a função de rede virtual em um data center e em um dispositivo uCPE
Interromper ou iniciar uma função de rede virtual ou uma VDU que faz parte dela
Pausar ou retomar uma função de rede virtual ou uma VDU que faz parte dela
Suspender ou cancelar a suspensão de uma função de rede virtual ou de uma VDU que faz parte dela
Reinicialização suave de uma função de rede virtual ou de uma VDU que faz parte dela
Reinicialização forçada de uma função de rede virtual ou de uma VDU que faz parte dela
Reimplementar uma função de rede virtual ou uma VDU que faz parte dela
Recuperação automática de uma função de rede virtual ou de uma VDU que faz parte dela
Gerenciar instantâneos de VDU
Criar um instantâneo de VDU
Restaurar as configurações de um VDU usando um instantâneo
Editar um instantâneo de VDU
Excluir um instantâneo de VDU

- Gerenciar funções de rede física
  - Selecionar a variação de uma função de rede física
  - Configurações básicas de uma função de rede física
- Configurar um serviço P2P
- Configurar um serviço P2M
- Configurar um serviço M2M
- Configurar uma rede compartilhada (OS 2 SHARED)
- Configurar um roteador virtual (OS vRouter)
- Configurar uma VLAN
- Configurar uma VXLAN
- Configurar uma rede plana
- Configurar uma UNI

Monitorar componentes da solução
- Especificar o servidor Zabbix
- Especificar o servidor proxy Zabbix
- Configurar o monitoramento do dispositivo CPE
- Visualizar os resultados de monitoramento
- Problemas de visualização
- Visualizar o status da solução e de seus componentes
- Visualizar logs
- Visualizar e excluir solicitações de serviço
- Enviar notificações de dispositivos CPE aos usuários
  - Especificar o servidor SMTP
  - Configurar notificações
- Selecionar o detalhamento do log do contêiner Docker
- Monitorar dispositivos CPE, VNF e PNF usando o SNMP
  - Configurar a conexão entre o gerenciador de SNMP e os agentes SNMP
  - Criar uma interceptação
  - Editar uma interceptação
  - Excluir uma interceptação
- Monitoramento de links

Construir uma rede SD-WAN entre dispositivos CPE
- Sobre a topologia Hub-and-Spoke
- Sobre as topologias Full-Mesh e Partial-Mesh
- Atribuir uma função a um dispositivo CPE
- Atribuir uma tag de topologia a um dispositivo CPE
- Configurar caminhos
- Gerenciar links
  - Visualizar estatísticas de um link
  - Atualizar automaticamente o custo do link com base na taxa de dados máxima da interface
  - Especificar o custo de um link
  - Ativar a atenuação
  - Ativar a Correção de erros de encaminhamento
  - Determinar o valor de MTU
  - Criptografia de tráfego
    - Ativar a criptografia de tráfego em um dispositivo CPE
    - Ativar a criptografia de tráfego em um link

- Gerenciamento de falhas de conectividade (CFM)
  - Ativar o CFM em um dispositivo CPE
  - Ativar o CFM em um link
- Gerenciar segmentos
  - Criar um caminho de Manual-TE
  - Editar um caminho de Manual-TE
  - Excluir um caminho de Manual-TE

Qualidade de serviço (QoS)
- Mecanismos de qualidade de serviço
- Marcação e remarcação de tráfego
- Gerenciar classes de tráfego
- Gerenciar classificadores de tráfego
  - Criar um classificador de tráfego
  - Editar um classificador de tráfego
  - Excluir um classificador de tráfego
- Gerenciar regras de qualidade de serviço
  - Criar uma regra de qualidade de serviço
  - Editar uma regra de qualidade de serviço
  - Excluir uma regra de qualidade de serviço
- Gerenciar restrições de Manual-TE
  - Criar uma restrição de Manual-TE
  - Editar uma restrição de Manual-TE
  - Excluir uma restrição de Manual-TE
- Gerenciar restrições de limite
  - Criar uma restrição de limite
  - Editar uma restrição de limite
  - Excluir uma restrição de limite
- Gerenciar regras de classificação de tráfego
  - Criar uma regra de classificação de tráfego
  - Editar uma regra de classificação de tráfego
  - Excluir uma regra de classificação de tráfego
- Gerenciar filtros de tráfego
  - Criar um filtro de tráfego
  - Editar um filtro de tráfego
  - Excluir um filtro de tráfego

Transmissão de tráfego entre dispositivos CPE e dispositivos cliente usando serviços de transporte
- Duplicação de pacotes de tráfego
- Cenário: direcionar o tráfego do aplicativo para um serviço de transporte
- Cenário: estabelecer conectividade L2 entre dispositivos CPE
- Cenário: gerenciar o tráfego do aplicativo de acordo com um SLA
- Gerenciar serviços de transporte ponto a ponto (P2P)
  - Criar um serviço P2P
  - Visualizar estatísticas de um serviço P2P
  - Visualizar e configurar a exibição de uma topologia de serviço P2P
  - Editar um serviço P2P
  - Reiniciar um serviço P2P
  - Excluir um serviço P2P

Gerenciar serviços de transporte ponto a multiponto (P2M)
- Criar um serviço P2M
- Visualizar estatísticas de um serviço P2M
- Visualizar a tabela MAC de um serviço P2M
- Visualizar e configurar a exibição de uma topologia de serviço P2M
- Editar um serviço P2M
- Reiniciar um serviço P2M
- Excluir um serviço P2M

Gerenciar serviços de transporte multiponto a multiponto (M2M)
- Criar um serviço M2M
- Visualizar as estatísticas de um serviço M2M
- Visualizar a tabela MAC de um serviço M2M
- Visualizar e configurar a exibição de uma topologia de serviço M2M
- Editar um serviço M2M
- Reiniciar um serviço M2M
- Excluir um serviço M2M

Gerenciar serviços de transporte multicast IP
- Criar um serviço multicast IP
- Visualizar as estatísticas de um serviço multicast IP
- Editar um serviço multicast IP
- Excluir um serviço multicast IP

Gerenciar serviços de transporte VPN L3
- Criar um serviço de VPN L3
- Gerenciar a tabela ARP de um serviço de VPN L3
  - Criar um registro estático na tabela ARP de um serviço de VPN L3
  - Editar um registro estático na tabela ARP de um serviço de VPN L3
  - Excluir um registro estático na tabela ARP de um serviço de VPN L3
- Visualizar a tabela de roteamento e encaminhamento de um serviço de VPN L3
- Editar um serviço de VPN L3
- Reiniciar um serviço de VPN L3
- Excluir um serviço de VPN L3

Gerenciar serviços de transporte em um modelo de instância SD-WAN
- Criar um serviço P2M ou M2M em um modelo de instância SD-WAN
- Criar um serviço de VPN L3 em um modelo de instância SD-WAN
- Editar um serviço de transporte em um modelo de instância SD-WAN
- Excluir um serviço de transporte em um modelo de instância SD-WAN

Gerenciar serviços de transporte em um modelo de CPE
- Adicionar um serviço de transporte a um modelo de CPE
- Editar um serviço de transporte em um modelo de CPE
- Excluir um serviço de transporte de um modelo de CPE

Espelhamento e encaminhamento de tráfego entre dispositivos CPE
- Gerenciar destinos de tráfego
  - Criar um destino de tráfego
  - Excluir um destino de tráfego
- Gerenciar serviços TAP
  - Criar um serviço TAP
  - Visualizar estatísticas de um serviço TAP

Editar um serviço TAP
Excluir um serviço TAP
Integração com a Kaspersky Unified Monitoring and Analysis Platform
Instalação do KUMA
Cenário: configuração do KUMA
Configuração do armazenamento no KUMA
Criação e configuração de um normalizador no KUMA para mensagens syslog
Configuração do correlacionador e de regras de correlação no KUMA
Tabela de referência para criar regras de correlação KUMA
Configuração de um coletor para eventos syslog no KUMA
Configuração do serviço de e-mail no KUMA
Configuração de regras de notificação no KUMA
Exemplos de configurações para pesquisas por eventos de chave no KUMA
Integração com o Kaspersky CyberSecurity for Networks
Contatar o Suporte Técnico
Como obter Suporte Técnico
Suporte Técnico através do Kaspersky CompanyAccount
Fontes de informações sobre a solução
Apêndices
Glossário
Controlador
CPE universal (uCPE)
Equipamento nas instalações do cliente (CPE)
Estratégia de transporte
Função de rede física (PNF)
Função de rede virtual (VNF)
Gateway SD-WAN
Gerenciador de funções de rede virtual (VNFM)
Gerenciador de infraestrutura virtual (VIM)
Instância SD-WAN
Locatário
Open vSwitch (OVS)
Orquestrador
Pacote da PNF
Pacote da VNF
Plano de controle
Plano de dados
Rede de longa distância definida por software (SD-WAN)
Rede definida por software (SDN)
Segurança de portas
Switch Operating System (SWOS)
Unidade de implementação virtual (VDU)
Informação sobre código de terceiros
Avisos de marca registrada

Ajuda do Kaspersky SD-WAN

Novos recursos

O que há de novo em cada versão do Kaspersky SD-WAN

Requisitos de hardware e software

Veja os requisitos de hardware e software

Introdução

- Implementar o Kaspersky SD-WAN
- Gerenciar a infraestrutura corporativa
- Gerenciar usuários e suas permissões de acesso
- Multilocação

Monitoramento e relatórios

- Configurar logs em dispositivos CPE
- Monitorar informações de pacotes de tráfego usando o protocolo NetFlow
- Diagnosticar dispositivos CPE
- Monitorar componentes da solução

Atualização

Atualizar o Kaspersky SD-WAN a partir de uma versão anterior

Recursos adicionais

- Gerenciar o firewall
- Qualidade de serviço (QoS)
- Espelhamento de tráfego

Apêndices

Obtenha informações sobre o Kaspersky SD-WAN em guias adicionais

Sobre o Kaspersky SD-WAN

O Kaspersky SD-WAN é usado para criar Redes de longa distância definidas por software (WAN definida por software; SD-WAN). Em redes SD-WAN, as rotas com a menor latência e a maior largura de banda são determinadas automaticamente. O tráfego é roteado usando a tecnologia SDN (Rede definida por software).

A *tecnologia SDN* separa o plano de controle do plano de dados e permite gerenciar a infraestrutura de rede por meio de um orquestrador (usando a interface da Web ou API). Separar o plano de controle do plano de dados possibilita *virtualizar funções de rede* (Virtualização de função de rede; NFV), de forma que funções de rede, como firewalls, roteadores e balanceadores de carga, são implementadas em equipamentos padrão. A virtualização da função de rede na solução é compatível com a especificação NFV MANO (Gerenciamento e orquestração de NFV) do Instituto Europeu de Normas de Telecomunicações (ETSI).

A construção de uma rede SD-WAN não depende de tecnologias de transporte. Também é possível enviar tráfego por diversos links com base nos requisitos do aplicativo em relação à largura de banda e à qualidade do serviço. Os seguintes tipos de rede underlay são compatíveis:

- Redes de transporte MPLS
- Links de banda larga para conexão com a Internet
- Linhas de comunicação dedicadas
- Conexões sem fio, incluindo 3G, 4G e LTE
- Links de satélite

A solução é destinada a provedores de serviços e organizações com uma grande rede de filiais. Ela substitui os roteadores padrão em redes distribuídas por dispositivos do tipo Equipamento nas Instalações do Cliente (CPE).

O Kaspersky SD-WAN permite:

- Gerenciamento inteligente de tráfego
- Configuração automática do dispositivo CPE
- Gerenciamento central de componentes da solução usando a interface da Web
- Monitoramento da rede
- Resposta automática a alterações nas políticas de QoS para atender aos requisitos dos aplicativos

A figura abaixo mostra um diagrama de uma rede SD-WAN criada usando a solução Kaspersky SD-WAN.

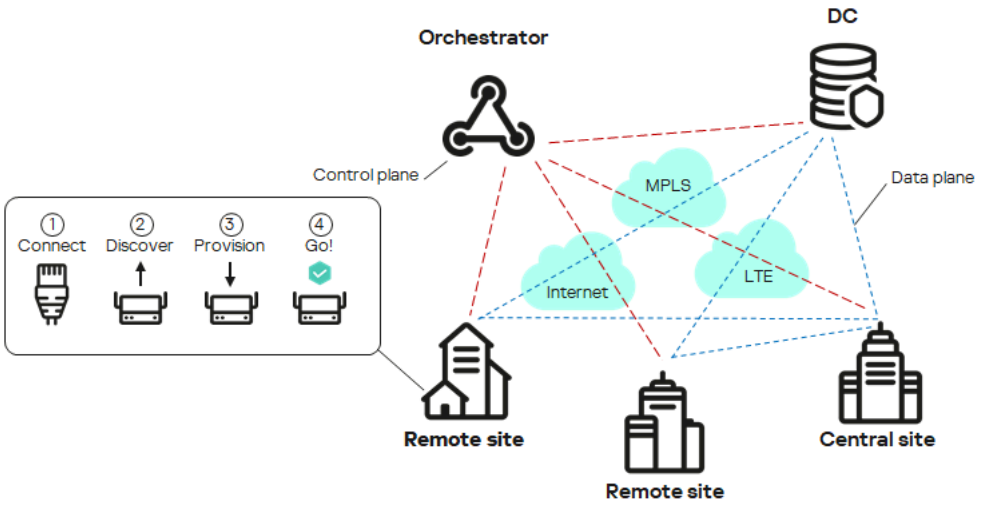


Diagrama de rede SD-WAN

Kit de distribuição

Para saber mais sobre como comprar a solução, acesse o site da Kaspersky (https://www.kaspersky.com) ou entre em contato com empresas parceiras.

O kit de distribuição inclui os seguintes componentes:

- knaas-installer_<informações da versão> no formato TAR.GZ (doravante também referido como o arquivo de instalação) para implementação da solução.
- Contêineres Docker para a implementação dos componentes do Kaspersky SD-WAN:
  - knaas-ctl
  - knaas-orc
  - knaas-www
  - knass-vnfm
  - knaas-vnfm-proxy
  - mockpnf

  É necessário baixar os seguintes contêineres do repositório comum do Docker:
  - mariaDB
  - mongo
  - redis
  - syslog-ng

- zabbix-proxy-mysql
- zabbix-server-mysql
- zabbix-web-nginx-mysql

- Firmware do dispositivo CPE.
- Um arquivo com o texto do Contrato de Licença do Usuário Final, que estipula os termos e as condições que você deve aceitar para usar a solução.
- Arquivos de Ajuda on-line do Kaspersky SD-WAN, que permitem ler a documentação sem uma conexão com a Internet.

O conteúdo do kit de distribuição pode diferir dependendo da região em que a solução é distribuída.

Requisitos de hardware e software

O Kaspersky SD-WAN tem os seguintes requisitos de hardware e software:

Os requisitos de hardware dependem do número de dispositivos CPE gerenciados (consulte os cenários de implementação recomendados abaixo). Se for necessário calcular os requisitos de hardware para um esquema de implementação específico com mais precisão, recomendamos entrar em contato com o Suporte Técnico da Kaspersky.

1. Recursos de computação recomendados para componentes da solução versão 2.4 ou posterior

A seguir estão as especificações compatíveis para instâncias do Kaspersky SD-WAN Orchestrator (ORC), Kaspersky SD-WAN Controller (CTL), o componente de monitoramento (MON) e o utilitário Kaspersky Deployment Toolkit (KDT); elas são válidas desde que sejam usados componentes e versões de software idênticos.

1.1. Orquestrador SD-WAN

Tabela 1. Definições do tipo de instância ORC

Tipo de instância	Número de dispositivos CPE	Especificações (aproximado)				
		CPU*	RAM	Tamanho de armazenamento**	IOPS de armazenamento**	Adaptador de rede
ORC pequeno	1000	16 núcleos	32 GB	256 GB	3.000	2 x 1 Gbps
ORC médio	5.000	24 núcleos	64 GB	512 GB	5.000	2 x 1 Gbps
ORC grande	10.000	16 núcleos	128 GB	1 TB	10.000	2 x 10 Gbps

*CPU sem Hyper-Threading. Recomendações:

- Xeon Silver 4314 para instâncias ORC pequenas
- Xeon Gold 5318Y, Xeon Gold 5418Y ou superior para instâncias ORC médias
- Xeon Gold 6414U, Xeon Gold 6438Y+ ou superior para instâncias ORC grandes

**SSD

1.2. Controlador SD-WAN

Tabela 2. Definições de tipo de instância CTL

Tipo de instância	Número de dispositivos CPE	Especificações (aproximado)				
		CPU*	RAM	Tamanho de armazenamento**	IOPS de armazenamento**	Adaptador de rede
CTL pequeno	250	16 núcleos	32 GB	64 GB	3.000	2 x 1 Gbps
CTL médio	500	24 núcleos	48 GB	128 GB	5.000	2 x 1 Gbps
CTL grande	1000	32 núcleos	64 GB	256 GB	10.000	2 x 10 Gbps

*CPU sem Hyper-Threading. Recomendações:

- Xeon Silver 4314 para instâncias CTL pequenas
- Xeon Gold 5318Y, Xeon Gold 5418Y ou superior para instâncias CTL médias
- Xeon Gold 6414U, Xeon Gold 6438Y+ ou superior para instâncias CTL grandes

**SSD

1.3. Componente de monitoramento SD-WAN

Tabela 3. Definições de tipo de instância MON

Tipo de instância	Número de dispositivos CPE	Especificações (aproximado)				
		CPU*	RAM	Tamanho de armazenamento**	IOPS de armazenamento**	Adaptador de rede
MON Pequeno	1.000	8 núcleos	16 GB	1 TB	3.000	2 x 1 Gbps
MON médio	5.000	24 núcleos	64 GB	5 TB	5.000	2 x 1 Gbps
MON grande	10.000	16 núcleos	96 GB	10 TB	10.000	2 x 10 Gbps

*CPU sem Hyper-Threading. Recomendações:

- Xeon Silver 4309Y para instâncias MON pequenas
- Xeon Gold 5318Y, Xeon Gold 5418Y ou superior para instâncias MON médias
- Xeon Gold 6414U, Xeon Gold 6438Y+ ou superior para instâncias MON grandes

**SSD, RAID 10

1.4. SD-WAN All-in-One

Uma instância do SD-WAN All-in-One (AIO) inclui os seguintes componentes de administração: Kaspersky SD-WAN Orchestrator (ORC), Kaspersky SD-WAN Controller (CTL) e o componente de monitoramento Kaspersky SD-WAN (MON). As seguintes especificações de instância são compatíveis:

Tabela 4. Definições de tipo de instância AIO

Tipo de instância	Número de dispositivos CPE	Especificações (aproximado)				
		CPU*	RAM	Tamanho de armazenamento**	IOPS de armazenamento**	Adaptador de rede
AIO pequeno	50	16 núcleos	32 GB	256 GB	3.000	1 Gbps
AIO médio	100	24 núcleos	48 GB	512 GB	5.000	2 x 1 Gbps
AIO grande	250	32 núcleos	64 GB	1024 GB	10.000	2 x 10 Gbps

1.5. Host para implementação de SD-WAN

Para implementar e atualizar os componentes de gerenciamento da solução nos cenários de Alta disponibilidade e Implementação distribuída, é necessário um host dedicado com o Kaspersky Deployment Toolkit (KDT).

Tabela 5. Definições de tipo de instância KDT

Cenário de implementação	Especificações (aproximado)				
	CPU*	RAM	Tamanho de armazenamento**	IOPS de armazenamento**	Adaptador de rede
Alta disponibilidade e Implementação distribuída	8 núcleos	16 GB	512 GB	5.000	1 Gbps

*CPU sem Hyper-Threading. Recomendações:

- Xeon Silver 4309Y para instâncias KDT

**SSD

2. Cenários de implementação do sistema de administração

2.1. Implementação independente

O cenário de implementação independente do sistema de administração Kaspersky SD-WAN é apenas para demonstração e não é recomendado para ambientes de produção.

2.2. Implementação da Alta disponibilidade

A implementação do sistema de administração Kaspersky SD-WAN em um cenário de Alta disponibilidade (HA) requer três instâncias AIO (HA3). Os requisitos de hardware das instâncias são especificados na Tabela 4. A tabela a seguir lista as recomendações de dimensionamento para a implementação de HA3.

Tabela 6. Requisitos de instâncias para implementação de HA3

Número de dispositivos CPE	Instância HA3
50	3 x AIO pequeno

100	3 x AIO médio
250	3 x AIO grande

2.3. Implementação distribuída

A implementação do sistema de administração Kaspersky SD-WAN em um cenário de Implementação distribuída requer três instâncias ORC dedicadas, três instâncias CTL dedicadas, três instâncias MON dedicadas e um host KDT.

Tabela 7. Requisitos de instâncias para implementação

Número de dispositivos CPE	ORC	CTL	MON	KDT
250	3 x ORC pequeno	3 x CTL pequeno	3 x MON pequeno	1 x KDT
500	3 x ORC pequeno	3 x CTL médio	3 x MON pequeno	1 x KDT
1.000	3 x ORC pequeno	3 x CTL grande	3 x MON pequeno	1 x KDT
2.500	3 x ORC pequeno	15 x CTL médio	3 x MON pequeno	1 x KDT
5.000	3 x ORC médio	30 x CTL médio	3 x MON médio	1 x KDT
7.500	3 x ORC médio	45 x CTL médio	3 x MON médio	1 x KDT
10.000	3 x ORC grande	60 x CTL médio	3 x MON grande	1 x KDT
20.000	6 x ORC grande	120 x CTL médio	6 x MON grande	1 x KDT
25.000	9 x ORC grande	150 x CTL médio	9 x MON grande	1 x KDT

3. Requisitos de soluções de terceiros

As seguintes soluções de terceiros são necessárias para implementar o Kaspersky SD-WAN:

- A plataforma Docker versão 1.5 ou posterior para a implementação de contêineres Docker de componentes da solução. Para mais informações, consulte a documentação oficial da plataforma Docker.
- O sistema de monitoramento Zabbix nas versões 5.0.26 ou 6.0.0. Para mais detalhes, consulte a documentação oficial da solução Zabbix.
- O serviço OpenStreetMap para visualização da topologia do serviço de transporte sobreposta em um mapa. Se a infraestrutura de sua organização não fornecer uma conexão com a Internet, é possível usar mapas offline. Os mapas offline ocupam espaço adicional em disco:
  - O mapa offline (central-fed-district-latest.osm.pbf) ocupa aproximadamente 100 GB.
  - Os dados de geocodificação ocupam aproximadamente 10 GB.

  Para obter informações detalhadas, consulte a documentação oficial do serviço OpenStreetMap.

Requisitos de sistema operacional

Os seguintes sistemas operacionais de 64 bits são compatíveis:

- Ubuntu 22.04.5 LTS.
- Astra Linux 1.8.5 (nível de segurança: "Orel").
- RED OS 7.3 "MUROM".

Requisitos para links entre nós de componentes da solução

Ao implementar o Kaspersky SD-WAN, é possível implementar diversos nós de componentes da solução. Os seguintes requisitos se aplicam aos links entre nós de componentes da solução:

- Requisitos para links entre nós do controlador:
  - Largura de banda: 1 Gbps
  - RTT (tempo de ida e volta): 200 ms ou menos
  - Perda de pacotes: 0%
- Requisitos para links entre nós do banco de dados MongoDB:
  - Largura de banda: 1 Gbps
  - RTT: 50 ms ou menos
  - Perda de pacotes: 0%
- Requisitos para links entre nós do banco de dados Redis:
  - Largura de banda: 1 Mbps
  - RTT: 50 ms ou menos
  - Perda de pacotes: 0%

Requisitos de navegador

Os seguintes navegadores podem ser usados para gerenciar a interface da Web do orquestrador:

- Google Chrome 100 ou posterior
- Firefox 100 ou posterior
- Microsoft Edge 100 ou posterior
- Opera 90 ou posterior
- Safari 15 ou posterior

Requisitos do dispositivo CPE

Os seguintes modelos de dispositivo CPE são compatíveis:

- KESR-M1-R-5G-2L-W
- KESR-M2-K-5G-1L-W
- KESR-M2-K-5G-1S
- KESR-M3-K-4G-4S
- KESR-M4-K-2X-1CPU
- KESR-M4-K-8G-4X-1CPU
- KESR-M5-K-8G-4X-2CPU
- KESR-M5-K-8X-2CPU

Dispositivos CPE do modelo KESR são baseados nas arquiteturas de processador x86 (Intel 80x86) e MIPS (Microprocessador sem estágios intertravados de pipeline).

Dispositivos CPE KESR M3–M5 têm adaptadores de rede Intel compatíveis com os transceptores Intel SFP. Para mais detalhes sobre os transceptores SFP compatíveis, use a Ferramenta de compatibilidade de produtos Intel

https://compatibleproducts.intel.com/ProductDetails?activeModule=Intel%C2%AE%20Ethernet#
(No território da Federação Russa, o link só pode ser acessado via VPN). Ao usar a Ferramenta de compatibilidade de produtos Intel, selecione uma das seguintes categorias de produtos:

- **500 Series** para visualizar transceptores SFP compatíveis com dispositivos CPE KESR M3.
- **700 Series** para visualizar transceptores SFP compatíveis com dispositivos CPE KESR M4–M5.

Os especialistas da Kaspersky realizaram testes para confirmar a funcionalidade dos dispositivos CPE ao fornecer o serviço de VPN L3 (consulte a tabela abaixo). Não foi usada DPI (Inspeção profunda de pacotes) nos dispositivos testados e a criptografia de tráfego foi desativada.

Hardware	Tamanho do arquivo (bytes)	Largura de banda (Mbps)
KESR-M1	IMIX (417)	30
	Grande (1300)	115
KESR-M2	IMIX (417)	165
	Grande (1300)	241
KESR-M3	IMIX (417)	805
	Grande (1300)	1150
KESR-M4	IMIX (417)	1430
	Grande (1300)	2870

Para obter informações detalhadas sobre as características de dispositivos CPE, consulte a página oficial da solução.

É possível implementar dispositivos uCPE em servidores com arquiteturas de processador x86 (Intel 80x86) ou ARM64.

Requisitos do dispositivo vCPE

O kit de distribuição inclui o seguinte firmware para a implementação de dispositivos vCPE:

- vKESR-M1
- vKESR-M2
- vKESR-M3
- vKESR-M4

Os seguintes ambientes de virtualização são compatíveis com dispositivos vCPE:

- VMware 7.0 ou posterior
- KVM com kernel versão 5.15 ou posterior

> Somente o ambiente de virtualização KVM original sem ferramentas de orquestração adicionais é compatível.

A tabela a seguir lista os requisitos de recursos virtuais para a implementação de dispositivos vCPE.

Firmware	CPU	RAM, GB	Disco, GB
vKESR-M1	2	0,5	1
vKESR-M2	4	8	1
vKESR-M3	12	16	1
vKESR-M4	24	32	1

Ao atualizar o Kaspersky SD-WAN da versão 2.2 para 2.3, certifique-se de que os dispositivos vCPE implementados anteriormente atendem aos requisitos da nova versão, após o que será possível atualizar os dispositivos vCPE usando o firmware vKESR-M1-5.

Garantir segurança

A segurança no Kaspersky SD-WAN é garantida no plano de dados, no plano de controle e no plano de orquestração. O nível de segurança da solução como um todo é determinado pelo nível de segurança de cada um desses planos, bem como pela segurança da interação entre eles. Os seguintes processos ocorrem em cada plano:

- Autenticação e autorização do usuário
- Uso de protocolos de gerenciamento seguros
- Criptografia do tráfego de controle
- Conexão segura de dispositivos CPE

Protocolos de gerenciamento seguros

Recomendamos o uso de HTTPS ao se comunicar com a rede SD-WAN através da interface da Web do orquestrador ou da API. É possível carregar seus próprios certificados para a interface da Web ou usar certificados autoassinados gerados automaticamente. A solução usa diversos protocolos para transmitir o tráfego de controle aos componentes (consulte a tabela abaixo).

Componentes de interação	Protocolo	Medidas de segurança adicionais
Orquestrador e controlador	gRPC	TLS é usado para autenticação e criptografia de tráfego entre o cliente e o servidor.
Orquestrador e dispositivo CPE	HTTPS	A verificação de certificado e um token são usados para autenticação e criptografia de tráfego entre o orquestrador e o dispositivo CPE.
Controlador e dispositivo CPE	OpenFlow 1.3.4	O TLS é usado para autenticação e criptografia de tráfego entre o controlador e o dispositivo CPE.

Conexão segura de dispositivos CPE

A solução usa os seguintes mecanismos para a conexão segura de dispositivos CPE:

- Descoberta de dispositivos CPE por DPIDs (identificadores de caminho de dados).
- Registro adiado. É possível selecionar o estado do dispositivo CPE após o registro bem-sucedido: **Ativado** ou **Desativado**. Um dispositivo CPE desativado deve ser ativado após certificar-se de que ele está instalado no local.
- Autenticação de dois fatores.

Uso de funções de rede virtual

É possível fornecer uma camada adicional de segurança com funções de rede virtual implementadas no data center e/ou em uCPEs. Por exemplo, o tráfego pode ser retransmitido de um dispositivo CPE para uma função de rede virtual que atua como firewall ou servidor proxy. As funções de rede virtual podem executar as seguintes funções de proteção de SD-WAN:

- Firewall de Próxima Geração (NGFW)
- Proteção contra ataques DDoS (negação de serviço distribuído)
- Sistema de Detecção de Intrusão (IDS) e Sistema de Prevenção de Intrusão (IPS)
- Antivírus
- Antispam
- Sistema de filtragem de conteúdo e filtragem de URL
- Sistema de DLP (Prevenção contra perda de dados) para evitar vazamentos de informações confidenciais
- Proxy da Web seguro

Novidades

O Kaspersky SD-WAN tem as seguintes funcionalidades novas e aprimoradas:

- A solução foi preparada para o início do procedimento de certificação do estado (aplica-se somente à Federação Russa)

  A certificação da solução Kaspersky SD-WAN confirmará a conformidade com os rígidos padrões de segurança impostos pelo estado e a capacidade de resistir a ameaças cibernéticas graves, fornecendo o mais alto nível de proteção aos sistemas de informação do estado (GIS), aos dados pessoais (ISPDN) e aos sistemas de controle industrial. Ao escolher esta solução, nossos clientes não apenas cumprem suas obrigações legais formais, mas também obtêm uma vantagem estratégica ao construir sua infraestrutura de TI com base em uma solução com um nível de segurança confirmado de forma independente.

- Proteção contra ataques de inundação SYN

  Apresentamos a proteção contra ataques de sobrecarga de recursos do servidor por meio de inundação de TCP SYN. Tais ataques visam tornar o dispositivo CPE indisponível para tráfego legítimo. A solução agora inclui um mecanismo interno que ajudará a impedir ataques desse tipo.

- Novo menu lateral

  O novo menu lateral é 26% mais amplo, o que facilita o gerenciamento da solução.

- Visualização de tabelas de sessão no orquestrador

  Antes, você precisava fazer login de forma manual em cada dispositivo CPE para visualizar as tabelas de sessão; agora você pode visualizar os parâmetros diretamente no orquestrador. Esse novo recurso facilita a solução de problemas.

- Apoio da comunidade BGP

  O Kaspersky SD-WAN agora é compatível com a comunidade BGP, o que permite o gerenciamento flexível de políticas de roteamento sem aumentar a complexidade da topologia: as informações sobre rotas são transportadas por tags de comunidade, que os CPEs usam para aplicar mecanismos de balanceamento.

- Registro aprimorado

  Cada evento de segurança agora tem critérios que indicam se ele é uma violação de segurança. Agora, as notificações sobre violações de segurança que ocorrem em CPEs e no orquestrador também podem ser enviadas para um coletor da Kaspersky Unified Monitoring and Analysis Platform (KUMA). Antes, os dados podiam ser enviados ao KUMA como um fluxo, requerendo uma classificação manual do que era ou não uma violação. Esse novo recurso melhora o controle e a segurança, além de facilitar o monitoramento da rede.

- Criptografia do syslog

  Agora você pode criptografar a comunicação do syslog (a criptografia de túnel ao enviar pela Internet não é eliminada), o que protege os registros quando eles são transmitidos para uma solução Kaspersky SIEM.

- QoS para tráfego de trânsito

  Dependendo da topologia da rede, alguns CPEs podem retransmitir o tráfego de trânsito. Agora você pode priorizar esse tráfego de trânsito para obter uma transmissão de rede e de tráfego mais eficientes. Antes, somente o tráfego principal podia ser priorizado.

- Filtragem de pacotes fragmentados

  Um novo mecanismo de processamento de tráfego de rede analisa pacotes IP e permite ou bloqueia pacotes fragmentados. Esse novo recurso melhora a segurança da rede enquanto aumenta o desempenho.

Limitações conhecidas

O Kaspersky SD-WAN tem as seguintes limitações:

- Limitações ao integrar a solução ao Kaspersky KSC/OSMP:
  - Disponível apenas para novas instalações
  - O console SSH não é compatível
  - O console VNC não é compatível
- As regras de firewall não levam em consideração tabelas de roteamento e encaminhamento virtual criadas pelo usuário da conta (não é possível especificar regras que correspondam a uma tabela de roteamento e encaminhamento virtual; em vez disso, use outros atributos, como interfaces, endereços IP).
- Quando as rotas estáticas são modificadas, o daemon FRR pode ser reiniciado.
- Alternar os modos do modem entre LTE e 3G (UMTS, CDMA, TD-SCDMA) pode causar uma lacuna nos gráficos de diagnóstico porque, para LTE, estão disponíveis os parâmetros RSSI, RSRQ, RSRP e SNR e, para 3G, apenas RSSI e ECIO.
- O SSH, o VNC e o console da Web não estão disponíveis no modo não-VNFM.

Arquitetura da solução

O Kaspersky SD-WAN inclui os seguintes componentes principais:

- Orquestrador

  Controla a infraestrutura da solução, funciona como orquestrador de NFV (NFVO) e gerencia serviços de rede e gerenciadores de VNF distribuídos (VNFMs). É possível gerenciar o orquestrador por meio da interface da Web ou da API REST ao usar sistemas externos northbound.

- Controlador

  Gerencia de forma centralizada a rede overlay:

  - Cria a topologia da rede.
  - Cria serviços de transporte.
  - Gerencia dispositivos CPE usando o protocolo OpenFlow.
  - Equilibra o tráfego entre links.
  - Monitora links e muda o tráfego automaticamente para um link de backup se o link principal falhar.

  Para implementar o controlador, é necessário implementar a função de rede física do controlador, contida no arquivo de instalação. O controlador é gerenciado pelo orquestrador.

- Dispositivos CPE

  São instalados em locais remotos para retransmitir o tráfego e formar uma malha SDN na forma de uma rede overlay. É possível atribuir a função de Gateway SD-WAN ou a função de dispositivo CPE padrão ao dispositivo CPE. Gateways SD-WAN estabelecem links com todos os dispositivos CPE padrão e outros Gateways SD-WAN. Dispositivos CPE padrão estabelecem links somente com Gateways SD-WAN. Por padrão, todos os dispositivos CPE têm a função de dispositivo CPE padrão.

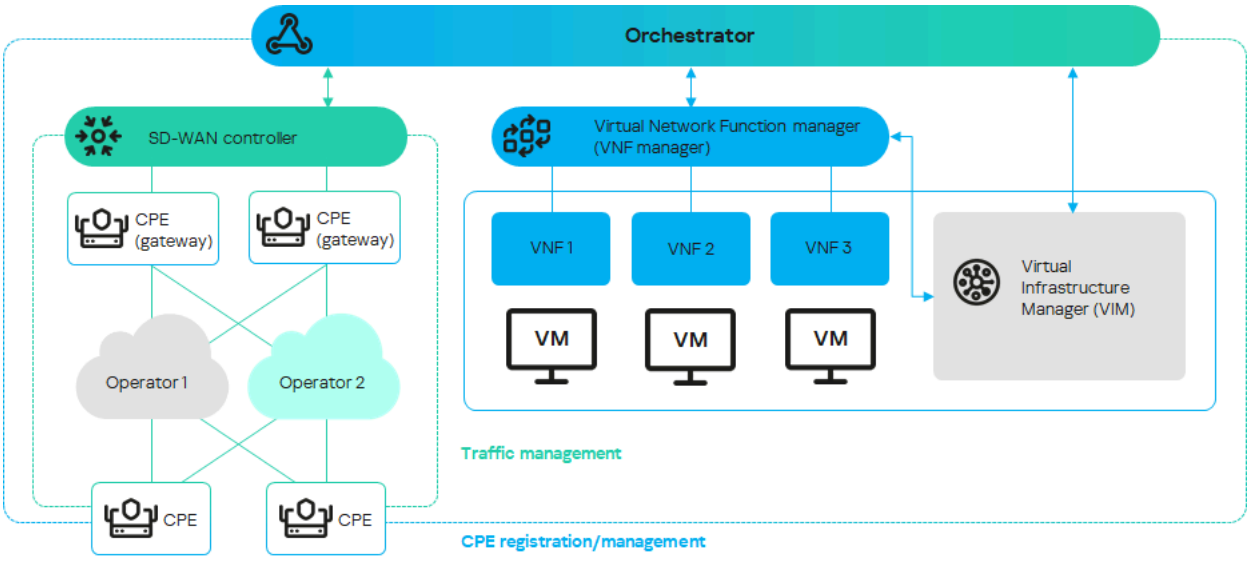
  Para que um link seja estabelecido entre dois dispositivos CPE padrão, é necessário atribuir a mesma tag de topologia a eles. É possível transformar um dispositivo CPE padrão em um dispositivo de trânsito para permitir que outros dispositivos CPE estabeleçam links através dele.

- VNFM (Gerenciador de funções de rede virtual)

  Gerencia o ciclo de vida das funções de rede virtual usando SSH, manuais do Ansible, scripts e atributos Cloud-init.

Se as funções de rede virtual forem usadas, a arquitetura da solução incluirá um Gerenciador de infraestrutura virtual (VIM) que gerencia recursos de computação, rede e armazenamento dentro da infraestrutura NFV. Um VIM conecta funções de rede virtual usando links, sub-redes e portas virtuais. A plataforma de nuvem OpenStack é usada como o VIM.

O Kaspersky SD-WAN tem uma arquitetura de microsserviço distribuída baseada em contêineres do Docker (veja a figura abaixo). Um controlador pode incluir um, três ou cinco nós. Para tolerância a falhas, implemente nós do controlador em máquinas virtuais ou servidores físicos separados. É possível especificar máquinas virtuais ou servidores físicos para implementação de nós do controlador ao implementar a solução, na seção `ctl` do arquivo de configuração.



Arquitetura do Kaspersky SD-WAN

Implementar o Kaspersky SD-WAN

Para implementar o Kaspersky SD-WAN, use o arquivo de instalação knaas-installer_<informações da versão> que faz parte do kit de distribuição. Antes de seguir com este procedimento, prepare um cenário de implementação da solução. Caso tenha algum problema ao preparar um cenário de implementação, recomendamos entrar em contato com o Suporte Técnico da Kaspersky.

Um cenário de implementação da solução consiste nas seguintes etapas:

1. **Preparar o dispositivo do administrador**

   Prepare o dispositivo do administrador para a implementação da solução. É possível usar uma máquina virtual local ou remota ou um computador pessoal como dispositivo do administrador. Ao implementar uma plataforma de teste do Kaspersky SD-WAN de acordo com o cenário de implementação tudo-em-um, é necessário usar uma máquina virtual como dispositivo do administrador.

2. **Garantir a conectividade de rede entre o dispositivo do administrador e os componentes da solução**

   Garanta a conexão de rede entre o dispositivo do administrador e as máquinas virtuais ou os servidores físicos nos quais deseja implementar os componentes do Kaspersky SD-WAN. Caso planeje implementar vários nós de componentes da solução, assegure-se de que os links entre máquinas virtuais ou servidores físicos atendam aos requisitos de hardware e software.

   > As máquinas virtuais ou os servidores físicos devem ser implementados em um segmento de rede confiável para evitar comprometer o tráfego transmitido.

3. **Gerar senhas manualmente**

   Se necessário, gere senhas manualmente para garantir a segurança dos componentes do Kaspersky SD-WAN e seus certificados SSL.

4. **Preparar o arquivo de configuração**

   Prepare o arquivo de configuração de acordo com o cenário de implementação escolhido. Encontre arquivos de configuração de exemplo para cenários de implementação típicos nos diretórios /inventory/external/pnf e /inventory/external/vnf do arquivo de instalação.

5. **Substituir os gráficos da interface da Web do orquestrador**

   Se necessário, substitua os gráficos da interface da Web do orquestrador. Por exemplo, substitua a imagem exibida em segundo plano quando um erro ocorre ao fazer login na interface da Web do orquestrador.

6. **Implementar o Kaspersky SD-WAN**

   Faça o seguinte no dispositivo do administrador:

   1. Aceite o Contrato de Licença do Usuário Final executando o seguinte comando:

      ```
      export KNAAS_EULA_AGREED="true"
      ```

   2. Acesse o diretório com o arquivo de instalação extraído.

3. Para implementar o Kaspersky SD-WAN no modo assistido, execute uma das seguintes ações:

   - Caso tenha gerado senhas manualmente, execute o comando:

     ```
     ansible-playbook -i inventory/generic -e "@< caminho para o arquivo de configuração >" -e "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
     ```

     Ao executar o comando, insira a senha da conta raiz e a senha mestra gerada.

   - Caso não tenha gerado senhas manualmente, execute o comando:

     ```
     ansible-playbook -i inventory/generic -e "@< caminho para o arquivo de configuração >" -e "@inventory/external/images.yml" -K knaas/knaas-install.yml
     ```

4. Para implementar o Kaspersky SD-WAN no modo autônomo, execute uma das seguintes ações:

   Recomendamos usar esse modo somente em um ambiente confiável, caso contrário, hackers podem interceptar suas senhas.

   - Caso tenha gerado senhas manualmente, execute o comando:

     ```
     ansible-playbook -i inventory/generic -e "@< caminho para o arquivo de configuração >" -e "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
     ```

   - Caso não tenha gerado senhas manualmente, execute o comando:

     ```
     ansible-playbook -i inventory/generic -e "@< caminho para o arquivo de configuração >" -e "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" knaas/knaas-install.yml
     ```

Os componentes do Kaspersky SD-WAN são implementados nas máquinas virtuais ou nos servidores físicos especificados no arquivo de configuração. Uma mensagem de implementação bem-sucedida é exibida no console do dispositivo do administrador.

Em caso de problemas de conexão de rede com uma das máquinas virtuais ou servidores físicos durante a implementação dos componentes da solução, uma mensagem de erro será exibida no console do dispositivo do administrador e a solução não será implementada. Nesse caso, restaure a conectividade de rede, limpe as máquinas virtuais ou os servidores físicos e, em seguida, execute o comando de implementação novamente.

Redundância de componentes da solução

Sobre esquemas de redundância para componentes da solução

O Kaspersky SD-WAN é compatível com dois cenários de implementação para componentes da solução:

- No cenário de implementação *N+1*, são implementados dois nós do componente da solução. Se um nó falhar, o segundo nó fornece a funcionalidade do componente da solução.

- No cenário de implementação *2N+1*, são implementados vários nós do componente da solução. Um nó é o principal e os demais são nós secundários. Se o nó principal falhar, um nó secundário escolhido aleatoriamente toma seu lugar. Esse esquema de redundância permite que os componentes da solução permaneçam operacionais mesmo após várias falhas seguidas.

A tabela abaixo lista os componentes da solução e os cenários de implementação aplicáveis a eles.

Componente da solução	Esquema de redundância
Banco de dados do sistema de monitoramento Zabbix	2N+1
Servidor Zabbix	N+1
Parte front-end do sistema de monitoramento Zabbix	N+1
Servidor proxy Zabbix	N+1
Banco de dados MongoDB	2N+1
Banco de dados Redis: • Servidor de réplica Redis • Sistema Redis Sentinel	2N+1
Controlador	2N+1
Parte de front-end da solução	N+1
Orquestrador	N+1
Gerenciador de funções de rede virtual	N+1
Proxy do Gerenciador de funções de rede virtual	N+1

É possível especificar o número de nós que deseja implementar para cada componente da solução no arquivo de configuração.

Ao definir as configurações de implementação para o banco de dados MongoDB ou o nó do controlador de acordo com o cenário de implementação 2N+1, o último nó especificado se torna o nó árbitro. O *nó árbitro* é vinculado a outros nós e usado para escolher o nó principal. Um nó que perdeu contato com o nó árbitro entra em modo de espera. Um dos nós que manteve contato com o nó árbitro se mantém ou se torna o nó principal. Um nó árbitro não pode se tornar um nó principal e não armazena dados.

Cenários de falha de nós de componentes da solução

A figura abaixo mostra um diagrama do Kaspersky SD-WAN implementado em três máquinas virtuais em um data center. O diagrama usa os seguintes símbolos:

- 'www' é a parte de front-end da solução

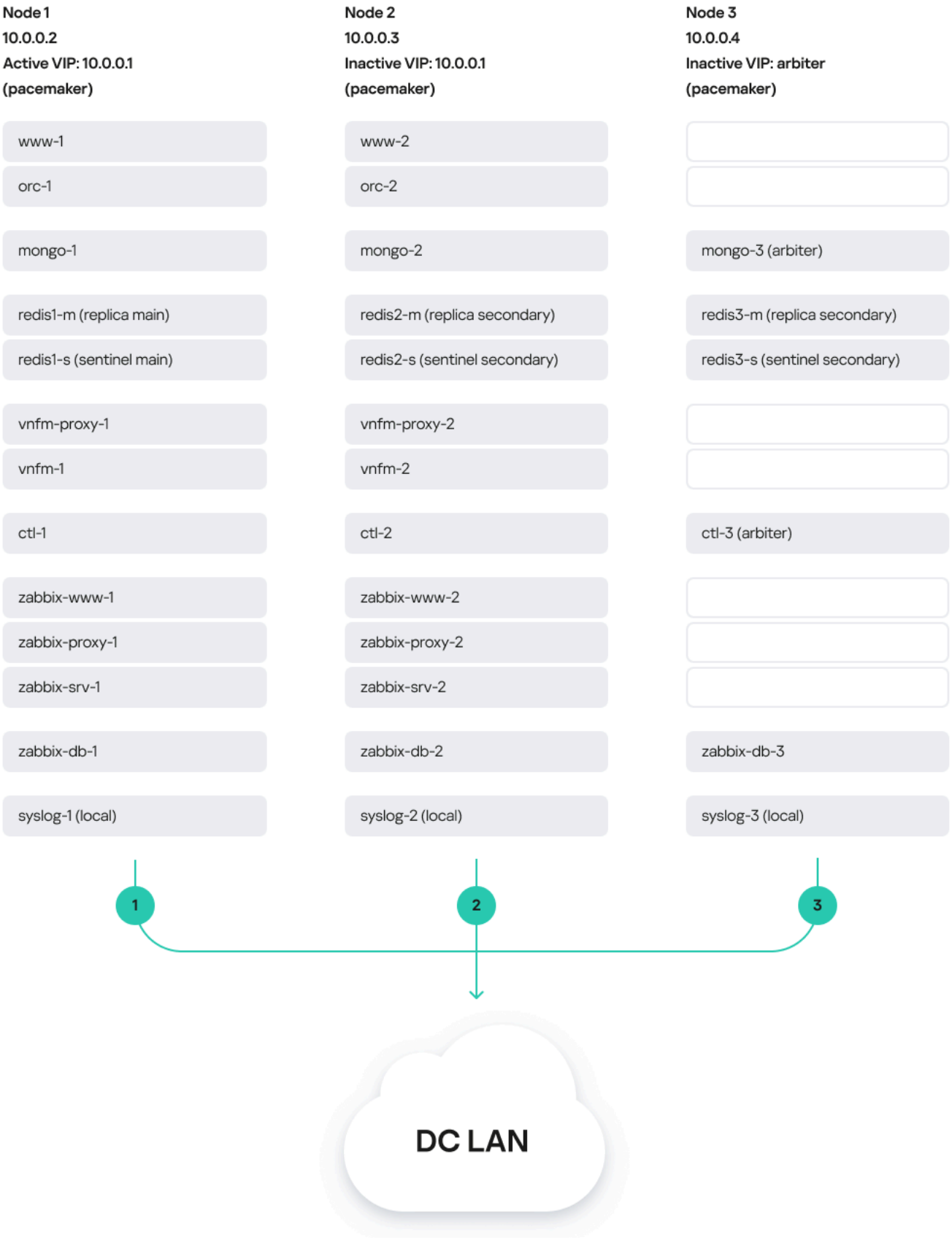
- 'orc' é o orquestrador

- 'mongo' é o banco de dados MongoDB

- 'redis-m' é um servidor de réplica Redis

- 'redis-s' é um sistema Redis Sentinel
- 'vnfm-proxy' é um proxy do gerenciador de funções de rede virtual
- 'vnfm' é um Gerenciador de funções de rede virtual
- 'ctl' é o controlador e seu banco de dados
- 'zabbix-www' é a parte de front-end do sistema de monitoramento Zabbix
- 'zabbix-proxy' é o servidor proxy Zabbix
- 'zabbix-srv' é o servidor Zabbix
- 'zabbix-db' é o banco de dados do sistema de monitoramento Zabbix
- 'syslog' é o servidor syslog

Usuários e dispositivos CPE obtêm acesso à interface da Web do orquestrador e à interface da Web do sistema de monitoramento Zabbix usando um endereço IP virtual. O endereço IP virtual é atribuído à máquina virtual 1.



Solução implementada em três máquinas virtuais

Neste cenário de implementação, os seguintes modos de falha são possíveis:

- **Falha da máquina virtual 1 ou de seu link**.

  Se a máquina virtual 1 ou seu link falhar, a solução permanece operacional. As seguintes alterações ocorrem no estado dos nós dos componentes da solução:

  - O endereço IP virtual é atribuído à máquina virtual 2.
  - O nó www-1 da parte de front-end da solução está indisponível; www-2 está disponível. A interface da Web do orquestrador é exibida no navegador.
  - O nó do orquestrador orc-1 está indisponível; orc-2 está disponível. A parte de back-end da solução é funcional, os usuários podem fazer login na interface da Web do orquestrador e gerenciá-la.
  - O nó mongo-1 do banco de dados MongoDB está indisponível; mongo-2 e mongo-3 estão disponíveis; mongo-2 se torna o nó principal, pois mongo-3 é o nó árbitro e não pode se tornar o nó principal. O orquestrador continua usando o banco de dados MongoDB.
  - Estado do banco de dados Redis:
    - O nó redis1-m do servidor de réplica Redis está indisponível; redis2-m e redis3-m estão disponíveis.
    - O nó redis1-s do sistema Redis Sentinel está indisponível; redis2-s e redis3-s estão disponíveis; redis2-s se torna o nó principal e atribui aleatoriamente o nó redis2-m ou redis3-m do servidor de réplica Redis como nó principal.

    O orquestrador continua usando o banco de dados Redis.
  - Estados do Gerenciador de funções de rede virtual:
    - O nó vnfm-proxy-1 do proxy do gerenciador de funções de rede virtual está indisponível; vnfm-proxy-2 está disponível.
    - O nó do Gerenciador de funções de rede virtual vnfm-1 está indisponível; vnfm-2 está disponível.

    Os consoles SSH dos componentes da solução estão operacionais.
  - O nó ctl-1 do controlador está indisponível; ctl-2 e ctl-3 estão disponíveis; ctl-2 se torna o nó principal, pois ctl-3 é o nó árbitro e não pode se tornar o nó principal. A conexão física entre dispositivos CPE é mantida.
  - Estado do sistema de monitoramento Zabbix:
    - O nó zabbix-www-1 da parte de front-end da solução está indisponível; zabbix-www-2 está disponível.
    - O nó zabbix-proxy-1 do servidor proxy Zabbix está indisponível; zabbix-proxy-2 está disponível.
    - O nó zabbix-srv-1 do servidor Zabbix está indisponível; zabbix-srv-2 está disponível.
    - O nó zabbix-db-1 do banco de dados do sistema de monitoramento Zabbix está indisponível; zabbix-db-2 está disponível.

    O sistema de monitoramento Zabbix está operacional.

- **Falha da máquina virtual 2 ou 3, ou de seu link**.

  Se a máquina virtual 2 ou 3 ou seu link falhar, os nós dos componentes da solução implementados na máquina virtual 1 permanecem como primários e a solução se mantém operacional.

- **Falha simultânea das máquinas virtuais 1 e 3 ou 2 e 3, ou de seus links**.

  Se as máquinas virtuais 1 e 3, as máquinas virtuais 2 e 3 ou seus links falharem simultaneamente, a solução para de funcionar. As seguintes alterações ocorrem no estado dos nós dos componentes da solução:

  - A interface da Web do orquestrador não é exibida no navegador. Os usuários não podem fazer login na interface da Web do orquestrador e gerenciá-la.
  - O sistema de monitoramento Zabbix para de funcionar.
  - A conexão de rede entre os dispositivos CPE e os dispositivos de rede conectados a eles é mantida; o tráfego continua a ser transmitido.
  - A conexão de rede nos serviços P2P e TAP é mantida.
  - A conexão de rede nos serviços P2M e M2M é mantida para sessões estabelecidas. Para novas sessões, a conexão de rede é mantida se, ao criar o serviço P2P ou M2M, na lista suspensa **Modo de aprendizado MAC**, você tiver selecionado **Aprender e inundar**.
  - Dispositivos CPE usam um mecanismo de compensação de reordenação para reduzir o número de pacotes duplicados em dispositivos de rede com conexão a dispositivos CPE.
  - A carga nos dispositivos CPE e na rede SD-WAN aumenta proporcionalmente ao número de dispositivos e links CPE.

  Se os links forem restaurados, a solução também é restaurada e retoma a operação normal.

  Se as máquinas virtuais 1 e 3 ou 2 e 3 falharem simultaneamente, a configuração dos componentes da solução será perdida. Para restaurar a configuração dos componentes da solução, entre em contato com o Kaspersky Professional Services.

- **Falha simultânea das máquinas virtuais 1 e 2**

  Se as máquinas virtuais 1 e 2 falharem simultaneamente, a configuração dos componentes da solução será perdida de forma irreversível, pois a máquina virtual 3 tem um árbitro que não armazena dados. Para evitar essa situação, recomendamos implementar bancos de dados e controladores em máquinas virtuais ou servidores físicos separados e fazer backups regulares.

Configurar o balanceamento de carga entre instâncias do orquestrador

Para melhorar o desempenho em ambientes de produção com muitos dispositivos CPE, ao implementar a solução, é possível criar várias instâncias do contêiner do orquestrador para distribuir a carga entre eles. Cada instância do contêiner do orquestrador pode servir até 5.000 dispositivos CPE.

As instâncias do contêiner são combinadas em *grupos de balanceamento*. Um grupo de balanceamento inclui um contêiner `www` e um a cinco contêineres do orquestrador. O número de grupos de balanceamento depende do esquema de implementação: 1 para um esquema tudo-em-um, 2 para um esquema de alta disponibilidade. Os nomes do contêiner seguem o padrão `orc-nm`, em que `n` representa o número do grupo de balanceamento e `m` representa o número ordinal da instância do contêiner no grupo, se o grupo incluir mais de uma instância. Exemplos: `orc-12` (contêiner do primeiro grupo de balanceamento, segunda instância); `orc-2` (a única instância de contêiner do segundo grupo de balanceamento).

Ao implementar o Kaspersky SD-WAN, os grupos de balanceamento podem ser implementados de duas formas:

- Implementando o contêiner `www` e os contêineres do orquestrador do grupo de balanceamento no mesmo nó.

  Para selecionar essa opção para implementação de um grupo de balanceamento, ao editar o arquivo de configuração, na variável `number_of_containers`, especifique o número de contêineres que devem ser implementados para o grupo de balanceamento no nó correspondente (de 1 a 5).

- O contêiner `www` e cada um dos contêineres do orquestrador do grupo de balanceamento são implementados em um nó separado.

  Essa opção pode ser usada para dimensionamento horizontal e uso mais eficiente de recursos. Para selecionar essa opção para a implementação de um grupo de balanceamento, ao editar o arquivo de configuração, na variável `ansible_host` das seções `orc_1` e `orc_2`, liste os nós relevantes da seção de `nós` nos quais deseja implementar instâncias dos contêineres do orquestrador. Apenas uma instância do contêiner do orquestrador pode ser implementada em cada nó especificado.

  Se mais de um nó for especificado na variável `ansible_host`, a configuração `number_of_containers` é ignorada.

Sobre o arquivo de instalação

O arquivo de instalação knaas-installer_<informações da versão> tem o formato TAR e é usado para a implementação da solução. É possível baixar o arquivo de instalação a partir do diretório raiz do kit de distribuição. O arquivo de instalação tem a seguinte estrutura:

Não recomendamos editar arquivos de sistema, pois isso pode causar erros ao implementar a solução.

- O arquivo ansible.cfg é um arquivo de sistema com configurações do Ansible.
- CHANGELOG.md é o log de alterações do arquivo no formato YAML.
- /docs contém a documentação do arquivo de instalação.
- /images contém imagens dos componentes da solução.
- /inventory:
  - /external:
    - /pnf contém exemplos de arquivos de configuração para cenários típicos de implementação da solução com o controlador como uma função de rede física.
    - /vnf contém exemplos de arquivos de configuração para cenários típicos de implementação da solução com o controlador como uma função de rede virtual.

- /generic contém arquivos de sistema comuns.
- /knaas contém arquivos de sistema com manuais para implementar a solução.
- /oem contém gráficos padrão da interface da Web do orquestrador.
- /pnfs contém funções de rede física para implementação de um, três ou cinco nós do controlador.
- README.md contém instruções para implementar a solução usando o arquivo de instalação.
- requirements.txt é um arquivo de sistema com os requisitos de Python.

Sobre os modos de ação assistido, autônomo e parcialmente assistido

Ao executar ações no dispositivo do administrador durante a implementação do Kaspersky SD-WAN, pode ser necessário inserir a senha raiz, bem como a senha mestra. A forma como as senhas são inseridas depende do modo no qual a ação é executada. Há suporte para os seguintes modos de ação:

- No modo assistido, um funcionário deve participar da ação. Para executar uma ação, é necessário inserir manualmente a senha raiz e a senha mestra. Este é o modo mais seguro que evita salvar qualquer senha no dispositivo do administrador.
- No modo autônomo, a ação é executada sem envolver um funcionário. Para executar uma ação, a senha raiz e a senha mestra são inseridas automaticamente. Nesse modo, é possível executar testes automatizados.

  Recomendamos usar esse modo somente em um ambiente confiável, caso contrário, hackers podem interceptar suas senhas.

- No modo parcialmente assistido, a ação é executada com o envolvimento parcial de um funcionário. Ao executar uma ação, é necessário inserir a senha raiz, mas a senha mestra é inserida automaticamente.

Preparar o dispositivo do administrador

É possível usar uma máquina virtual local ou remota ou um computador pessoal como dispositivo do administrador. Ao implementar uma plataforma de teste do Kaspersky SD-WAN de acordo com o cenário de implementação tudo-em-um, é necessário usar uma máquina virtual como dispositivo do administrador.

Caso tenha algum problema ao preparar o dispositivo do administrador, recomendamos entrar em contato com o Suporte Técnico da Kaspersky.

Para preparar o dispositivo do administrador:

1. Certifique-se de que o dispositivo do administrador atenda aos requisitos de hardware e software.

2. Certifique-se de que a mesma conta raiz seja usada no dispositivo do administrador e nas máquinas virtuais ou servidores físicos nos quais deseja implementar os componentes do Kaspersky SD-WAN. Após implementar a solução, é possível usar uma conta raiz diferente nas máquinas virtuais ou nos servidores físicos.

3. Baixe o arquivo de instalação knaas-installer_<informações da versão> a partir do diretório raiz do kit de distribuição e extraia o arquivo de instalação no dispositivo do administrador.

4. Acesse o diretório com o arquivo de instalação extraído e prepare o dispositivo do administrador:

   a. Certifique-se de que a ferramenta de gerenciamento de pacotes pip esteja instalada executando o comando:

   ```
   python3 -m pip -V
   ```

   b. Se a ferramenta de gerenciamento de pacotes pip não estiver presente, execute uma das seguintes operações:

   - Se o dispositivo do administrador estiver executando o Ubuntu:

     ```
     apt-get install python3-pip
     ```

   - Se o dispositivo do administrador estiver executando o RED OS 8:

     ```
     yum install python3-pip
     ```

   c. Instale a ferramenta Ansible e suas dependências:

   ```
   python 3 -m pip install -U --user -r requirements.txt
   ```

   d. Atualize a variável PATH:

   1. `echo 'export PATH=$PATH:$HOME/.local/bin' >> ~/.bashrc`
   2. `source ~/.bashrc`

   e. Verifique se a ferramenta Ansible está pronta para uso:

   ```
   ansible --version
   ```

   f. Instale os pacotes do sistema operacional para a implementação do Kaspersky SD-WAN no dispositivo do administrador:

   ```
   ansible-playbook -K knaas/utilities/toolserver_prepare/bootstrap.yml
   ```

   Insira a senha raiz ao executar o comando.

   Só é necessário concluir esta etapa ao implementar a solução pela primeira vez.

5. Certifique-se de que o dispositivo do administrador esteja pronto para uso:

   a. Reinicie o dispositivo do administrador.

   b. Acesse o arquivo de instalação extraído e inicie a verificação automática do dispositivo do administrador:

   ```
   ansible-playbook knaas/utilities/pre-flight.yml
   ```

6. Para implementar o Kaspersky SD-WAN em diversas máquinas virtuais ou servidores físicos:

   a. Certifique-se de que as chaves SSH tenham sido geradas no dispositivo do administrador. Se não existiram chaves SSH, gere-as.

   b. Coloque as chaves SSH em máquinas virtuais ou servidores físicos:

      ```
      ssh-copy-id user@< endereço IP da máquina virtual ou servidor físico >
      ```

   Caso esteja implementando uma plataforma de teste do Kaspersky SD-WAN de acordo com o cenário de implementação tudo-em-um, ignore esta etapa.

O dispositivo do administrador está preparado para a implementação do Kaspersky SD-WAN.

Gerenciar senhas

As senhas ajudam a garantir a segurança dos componentes do Kaspersky SD-WAN implementados. É possível gerar as senhas manualmente. Caso as senhas não sejam geradas manualmente, elas serão geradas automaticamente ao implementar a solução.

As senhas estão contidas nos seguintes arquivos:

- keystore.yml contém senhas de componentes do Kaspersky SD-WAN e seus certificados SSL.
- vault_password.txt contém a senha mestra.

Recomendamos armazenar os arquivos de senha em um diretório protegido pois eles podem ser usados para obter acesso à solução implementada.

Após a implementação, as senhas geradas são colocadas automaticamente nos contêineres Docker dos componentes do Kaspersky SD-WAN. Os componentes da solução trocam senhas ao interagir entre si.

Gerar senhas manualmente

Para gerar as senhas manualmente:

1. Crie o diretório /passwords no dispositivo do administrador. Especifique o caminho para o diretório criado na seção `externa` do arquivo de configuração usando a configuração `vault_password_dirname`.
2. Crie um arquivo keystore.yml e, nesse arquivo, especifique as senhas usando as seguintes configurações:
   - `ZABBIX_DB_SECRET` é a senha raiz do banco de dados do sistema de monitoramento Zabbix.
   - `MONGO_ADMIN_SECRET` é a senha do administrador do banco de dados MongoDB.
   - `MONGO_USER_SECRET` é a senha do usuário do banco de dados MongoDB. Essa senha é usada pelo orquestrador.
   - `CTL_CERT_SECRET` é a senha do certificado SSL do controlador.

- `ORC_CERT_SECRET` é a senha do certificado SSL do orquestrador.
- `ORC_ENC_SECRET` é a senha para criptografar dados confidenciais no banco de dados MongoDB. Comprimento mínimo: 32 caracteres.
- `VNFM_CERT_SECRET` é a senha do certificado SSL do VNFM.

> Para todas as senhas, exceto `ORC_ENC_SECRET`, recomendamos especificar pelo menos 16 caracteres.

3. Crie o arquivo vault_password.txt e, nele, especifique a senha mestra.
4. Criptografe o arquivo keystore.yml:
   - Para criptografar o arquivo keystore.yml no modo assistido:
     ```
     ansible-vault encrypt --ask-vault-pass keystore.yml
     ```
   - Para criptografar o arquivo keystore.yml no modo autônomo:
     ```
     ansible-vault encrypt --vault-password-file vault_password.txt keystore.yml
     ```

As senhas são geradas e criptografadas.

Alterar senhas

Para alterar as senhas:

1. Descriptografe o arquivo keystore.yml:
   - Para descriptografar o arquivo keystore.yml no modo assistido:
     ```
     ansible-vault decrypt --vault-password-file vault_password.txt keystore.yml
     ```
   - Para descriptografar o arquivo keystore.yml no modo autônomo:
     ```
     ansible-vault encrypt --ask-vault-pass keystore.yml
     ```
2. Altere as seguintes senhas no arquivo keystore.yml:
   - `ZABBIX_DB_SECRET` é a senha raiz do banco de dados do sistema de monitoramento Zabbix.
   - `MONGO_ADMIN_SECRET` é a senha do administrador do banco de dados MongoDB.
   - `MONGO_USER_SECRET` é a senha do usuário do banco de dados MongoDB. Essa senha é usada pelo orquestrador.
   - `CTL_CERT_SECRET` é a senha do certificado SSL do controlador.
   - `ORC_CERT_SECRET` é a senha do certificado SSL do orquestrador.
   - `ORC_ENC_SECRET` é a senha para criptografar dados confidenciais no banco de dados MongoDB. Comprimento mínimo: 32 caracteres.
   - `VNFM_CERT_SECRET` é a senha do certificado SSL do VNFM.

Para todas as senhas, exceto `ORC_ENC_SECRET`, recomendamos especificar pelo menos 16 caracteres.

3. Criptografe o arquivo keystore.yml:

   - Para criptografar o arquivo keystore.yml no modo assistido:

     ```
     ansible-vault encrypt --ask-vault-pass keystore.yml
     ```

   - Para criptografar o arquivo keystore.yml no modo autônomo:

     ```
     ansible-vault encrypt --vault-password-file vault_password.txt keystore.yml
     ```

   As senhas são alteradas e criptografadas.

Preparar o arquivo de configuração

Especifique as configurações de implementação do Kaspersky SD-WAN no arquivo de configuração YAML no dispositivo do administrador. O caminho para o arquivo de configuração deve ser especificado ao implementar a solução. Encontre arquivos de configuração de exemplo para cenários de implementação típicos nos diretórios inventory/external/pnf e inventory/external/vnf do arquivo de instalação.

O arquivo de configuração consiste em duas seções principais:

- A seção `nodes` especifica máquinas virtuais ou servidores físicos para a implementação dos componentes do Kaspersky SD-WAN. Ao implementar a solução em máquinas virtuais ou servidores físicos, as regras de iptables para interação entre os componentes da solução são geradas automaticamente.
- A seção `external` especifica as configurações de implementação do Kaspersky SD-WAN.

Não recomendamos alterar as configurações padrão.

A seção `nodes` tem a seguinte estrutura:

Seção/configuração			Descrição
`node_< número da máquina virtual ou servidor físico >`			Configurações de implementação da máquina virtual ou servidor físico.
	`ip`		Endereço IP da máquina virtual ou servidor físico. Insira um valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126`
	`vip`		Endereço IP virtual da máquina virtual ou servidor físico. Insira um valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` Essa configuração deve ser especificada para todas as máquinas virtuais ou servidores físicos nos quais se planeja usar endereços IP virtuais.
	`knaas_aio_int`		Configurações para conectar contêineres Docker de componentes do Kaspersky SD-WAN à rede virtual local da máquina virtual ou servidor físico.
		`base`	Os primeiros três octetos do endereço IP da rede virtual local. Valor padrão: `10.11.11`. Insira um valor no formato `XXX.XXX.XXX`, por exemplo: `192.168.110` É possível alterar os três primeiros octetos do endereço IP padrão se eles se sobrepuserem ao espaço de endereço.
		`mode`	Modo de operação da rede virtual local. Valores possíveis: • `bridge` significa que uma ponte Linux é criada na máquina virtual ou servidor físico. Os contêineres Docker estabelecem uma conexão com a ponte Linux por meio de uma rede L3 usando NAT e iptables. • `vlan` significa que os contêineres Docker estabelecem uma conexão com a interface da máquina virtual ou servidor físico por meio de uma rede L2 usando o driver macvlan. Recomendamos escolher esta opção apenas ao usar uma rede L2 confiável, pois, nesse caso, nenhum firewall é utilizado na máquina virtual ou no servidor físico.
		`iface`	Nome da máquina virtual ou interface do servidor físico para conexão de contêineres Docker através da rede L2, por exemplo: `enp6s0` Esse parâmetro deve ser especificado se para `mode`, você escolheu `vlan`.
		`vlan`	Tag VLAN da rede L2. Insira um valor no intervalo de 1 a 4095. Se você não quiser usar uma tag VLAN, insira `0`. Esse parâmetro deve ser especificado se para `mode`, você escolheu `vlan`.
	`knaas_os_man`		Configurações para conectar contêineres Docker de componentes do Kaspersky SD-WAN à rede virtual de gerenciamento ou ao servidor físico da máquina virtual.
		`base`	Os três primeiros octetos do endereço IP da rede virtual de gerenciamento. Valor padrão: `10.11.11`. Insira um valor no formato `XXX.XXX.XXX`, por exemplo: `192.168.110` É possível alterar os três primeiros octetos do endereço IP padrão se eles se sobrepuserem ao espaço de endereço.
		`mode`	Modo de operação da rede virtual de gerenciamento. Valores possíveis: • `bridge` significa que uma ponte Linux é criada na máquina virtual ou servidor físico. Os contêineres Docker estabelecem uma conexão com a ponte Linux por meio de uma rede L3 usando NAT e iptables. • `vlan` significa que os contêineres Docker estabelecem uma conexão com a interface da máquina virtual ou servidor físico por meio de uma rede L2 usando o driver macvlan. Recomendamos escolher esta opção apenas ao usar uma rede L2 confiável, pois, nesse caso, nenhum firewall é utilizado na máquina virtual ou no servidor físico.
		`iface`	Nome da máquina virtual ou interface do servidor físico para conexão de contêineres Docker através da rede L2, por exemplo: `enp6s0` Esse parâmetro deve ser especificado se para `mode`, você escolheu `vlan`.
		`vlan`	Tag VLAN da rede L2. Insira um valor no intervalo de 1 a 4095. Se você não quiser usar uma tag VLAN, insira `0`. Esse parâmetro deve ser especificado se para `mode`, você escolheu `vlan`.

A seção `external` tem a seguinte estrutura:

Seção/configuração			Descrição
`vault_passwords_dirname`			Caminho para o diretório /passwords no dispositivo do administrador com senhas geradas manualmente. Se as senhas não forem geradas manualmente, elas serão geradas de forma automática durante a implementação da solução e colocadas no diretório /passwords do arquivo de instalação extraído no dispositivo do administrador.
`ansible_user`			Nome da conta de usuário no dispositivo do administrador e em máquinas virtuais ou servidores físicos para executar manuais durante a implementação da solução.
`SSL`			Configurações de certificados SSL dos componentes do Kaspersky SD-WAN.
	`san_list`		Informações adicionadas aos certificados SSL.

		`ip`	Endereços IP adicionados aos certificados SSL. Especifique uma lista de valores no formato `XXX.XXX.XXX.XXX`, por exemplo:
			`ip`
			`- 192.168.2.0`
			`- 192.168.2.1`

		`dns`	Nomes de domínio adicionados aos certificados SSL. Especifique uma lista de valores, por exemplo:
			`dns:`
			`- sdwan.kaspersky.com`
			`- kaspersky.sdwan.com`

	`path_local`		Caminho para o diretório no dispositivo do administrador que contém certificados SSL gerados manualmente. Se os certificados SSL não forem gerados manualmente, eles serão gerados de forma automática durante a implementação da solução e colocados no diretório /ssl do arquivo de instalação extraído no dispositivo do administrador.
	`path_remote`		Caminho para o diretório nas máquinas virtuais ou servidores físicos que contém certificados SSL gerados manualmente. Se os certificados SSL não forem gerados manualmente, eles serão gerados de forma automática durante a implementação da solução e colocados no diretório /ssl em máquinas virtuais ou servidores físicos.
`syslog`			Configurações do servidor syslog.
	`docker_memory_limit`		Quantidade de RAM, em megabytes, para contêineres Docker do servidor syslog.
	`max_log_size`		Quantidade de RAM, em gigabytes, para logs do servidor syslog.
	`state`		Implementação de um servidor syslog em máquinas virtuais ou servidores físicos. Valores possíveis: • `enabled` • `disabled`
`zabbix`			Configurações do sistema de monitoramento Zabbix. Para mais detalhes, consulte a documentação oficial da solução Zabbix.

`syslog_server_address`	Endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviam logs. O valor é especificado no formato `<protocolo>://<endereço do host>:<número da porta>`. Você pode especificar o endereço IP ou FQDN do host como o endereço do host.
	Exemplos:
	`udp://192.168.2.15:1514`
	`tcp+tls://my-syslog-server:1514`
	Se a variável `secure_syslog` estiver definida como `true`, você precisará especificar `tcp+tls` como o prefixo do protocolo, por exemplo:
	`tcp+tls://192.168.2.15:1514`
	Se você quiser usar um coletor KUMA como servidor syslog, especifique o endereço do host no formato FQDN.
	Especifique as configurações do servidor syslog na seção `syslog`.

`secure_syslog`	Ativa ou desativa a criptografia de mensagens do syslog enviadas pelo contêiner do Docker. Valores possíveis: • `true` • `false` Valor padrão: `false`. Se definido como `false`, as mensagens do syslog são enviadas como texto sem formatação via UDP. Se definido como `true`, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável `syslog_server_ca_cert_file_path`.
`syslog_server_ca_cert_file_path`	O caminho absoluto do arquivo de certificado CA usado para assinar o certificado do servidor syslog. Necessário se `secure_syslog` estiver definido como `true`.
`syslog_format`	Formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis: `rfc3164` para formato compatível com RFC 3164. `rfc5424` para formato compatível com RFC 5424. `rfc5424micro` para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos. Se você quiser usar um coletor KUMA como servidor syslog, especifique `rfc3164`.
`db_docker_memory_limit`	Quantidade de RAM, em megabytes, para contêineres Docker do banco de dados do sistema de monitoramento Zabbix.
`srv_docker_memory_limit`	Quantidade de RAM, em megabytes, para contêineres Docker do servidor Zabbix.
`www_docker_memory_limit`	Quantidade de RAM, em megabytes, para contêineres Docker do front-end do sistema de monitoramento Zabbix.
`proxy_docker_memory_limit`	Quantidade de RAM, em megabytes, para contêineres Docker do servidor proxy Zabbix.
`cachesize`	Quantidade de RAM, em gigabytes, para o cache do sistema de monitoramento Zabbix. Insira um valor no formato `<gigabytes>G`, por exemplo: `8G`
`zabbix_<1-3>`	Configurações de implementação dos nós do sistema de monitoramento Zabbix. É possível implementar um nó do sistema de monitoramento Zabbix sem alta disponibilidade ou três nós com alta disponibilidade.

		`ansible_host`	Endereço IP da máquina virtual ou servidor físico da seção de `nós` para a implementação do sistema de monitoramento Zabbix. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` • Variável Ansible, por exemplo: `{{ nodes.node_1.ip }}`
		`db`	Configurações de implementação do banco de dados do sistema de monitoramento Zabbix.
		`inventory_hostname`	Nome do host do banco de dados do sistema de monitoramento Zabbix. Valor padrão: `zabbix-db-<1-3>`.
		`state`	Implementação do banco de dados do sistema de monitoramento Zabbix em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`srv`	Configurações de implementação do servidor Zabbix. Ao implementar três nós do sistema de monitoramento Zabbix, só é necessário especificar essas configurações para dois dos nós.
		`inventory_hostname`	Nome do host do servidor Zabbix. Valor padrão: `zabbix-srv-<1-3>`.
		`state`	Implementação do servidor Zabbix em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`www`	Configurações de implementação da parte de front-end do sistema de monitoramento Zabbix. Ao implementar três nós do sistema de monitoramento Zabbix, só é necessário especificar essas configurações para dois dos nós.
		`inventory_hostname`	Nome do host da parte de front-end do sistema de monitoramento Zabbix. Valor padrão: `zabbix-www-<1-3>`.
		`state`	Implementação da parte de front-end do sistema de monitoramento Zabbix em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`proxy`	Configurações de implementação do servidor proxy Zabbix. Ao implementar três nós do sistema de monitoramento Zabbix, só é necessário especificar essas configurações para dois dos nós.
		`inventory_hostname`	Nome do host do servidor proxy Zabbix. Valor padrão: `zabbix-proxy-<1-3>`.
		`state`	Implementação do servidor proxy Zabbix em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
`mongo`			Configurações do banco de dados MongoDB. Para mais detalhes, consulte a documentação oficial do banco de dados MongoDB.

	`syslog_server_address`		Endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviam logs. O valor é especificado no formato `<protocolo>://<endereço do host>:<número da porta>`. Você pode especificar o endereço IP ou FQDN do host como o endereço do host.
			Exemplos:
			`udp://192.168.2.15:1514`
			`tcp+tls://my-syslog-server:1514`
			Se a variável `secure_syslog` estiver definida como `true`, você precisará especificar `tcp+tls` como o prefixo do protocolo, por exemplo:
			`tcp+tls://192.168.2.15:1514`
			Se você quiser usar um coletor KUMA como servidor syslog, especifique o endereço do host no formato FQDN.
			Especifique as configurações do servidor syslog na seção `syslog`.

	`secure_syslog`		Ativa ou desativa a criptografia de mensagens do syslog enviadas pelo contêiner do Docker. Valores possíveis: • `true` • `false` Valor padrão: `false`. Se definido como `false`, as mensagens do syslog são enviadas como texto sem formatação via UDP. Se definido como `true`, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`		O caminho absoluto do arquivo de certificado CA usado para assinar o certificado do servidor syslog. Necessário se `secure_syslog` estiver definido como `true`.
	`syslog_format`		Formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis: `rfc3164` para formato compatível com RFC 3164. `rfc5424` para formato compatível com RFC 5424. `rfc5424micro` para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos. Se você quiser usar um coletor KUMA como servidor syslog, especifique `rfc3164`.
	`docker_memory_limit`		Quantidade de RAM, em megabytes, para contêineres Docker do banco de dados MongoDB.
	`mongo_<1-3>`		Configurações de implementação dos nós do banco de dados MongoDB. É possível implementar um nó do banco de dados MongoDB sem alta disponibilidade ou três nós com alta disponibilidade. Ao implementar três nós do banco de dados MongoDB, o último se torna o nó de arbitragem.
		`inventory_hostname`	Nome do host do banco de dados MongoDB. Valor padrão: `mongo-<1-3>`
		`state`	Implementação do banco de dados MongoDB em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`ansible_host`	Endereço IP da máquina virtual ou servidor físico da seção `nodes` para a implementação do banco de dados MongoDB. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` • Variável Ansible, por exemplo: `{{ nodes.node_1.ip }}`
`redis`			Configurações do banco de dados Redis. Para mais detalhes, consulte a documentação oficial do banco de dados Redis.

`syslog_server_address`		Endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviam logs. O valor é especificado no formato `<protocolo>://<endereço do host>:<número da porta>`. Você pode especificar o endereço IP ou FQDN do host como o endereço do host.
		Exemplos:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Se a variável `secure_syslog` estiver definida como `true`, você precisará especificar `tcp+tls` como o prefixo do protocolo, por exemplo:
		`tcp+tls://192.168.2.15:1514`
		Se você quiser usar um coletor KUMA como servidor syslog, especifique o endereço do host no formato FQDN.
		Especifique as configurações do servidor syslog na seção `syslog`.

`secure_syslog`		Ativa ou desativa a criptografia de mensagens do syslog enviadas pelo contêiner do Docker. Valores possíveis: • `true` • `false` Valor padrão: `false`. Se definido como `false`, as mensagens do syslog são enviadas como texto sem formatação via UDP. Se definido como `true`, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável `syslog_server_ca_cert_file_path`.
`syslog_server_ca_cert_file_path`		O caminho absoluto do arquivo de certificado CA usado para assinar o certificado do servidor syslog. Necessário se `secure_syslog` estiver definido como `true`.
`syslog_format`		Formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis: `rfc3164` para formato compatível com RFC 3164. `rfc5424` para formato compatível com RFC 5424. `rfc5424micro` para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos. Se você quiser usar um coletor KUMA como servidor syslog, especifique `rfc3164`.
`docker_memory_limit`		Quantidade de RAM, em megabytes, para contêineres Docker do banco de dados Redis.
`redis_<1-3>m`		Configurações de implementação para nós do servidor de réplica Redis. É possível implementar um nó do servidor de réplica Redis sem alta disponibilidade ou três nós com alta disponibilidade.
	`inventory_hostname`	Nome do host do servidor de réplica Redis. Valor padrão: `redis-<1-3>m`.
	`state`	Implementação do servidor de réplica Redis em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
	`ansible_host`	Endereço IP da máquina virtual ou servidor físico da seção `nodes` para a implementação do servidor de réplica Redis. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` • Variável Ansible, por exemplo: `{{ nodes.node_1.ip }}`
`redis_<1-3>s`		Configurações de implementação de nós do sistema Redis Sentinel. Ao implementar três nós do servidor de réplica Redis com alta disponibilidade, também é necessário implementar três nós do sistema Redis Sentinel.

		`inventory_hostname`	Nome do host do sistema Redis Sentinel. Valor padrão: `redis-<1-3>s`.
		`state`	Implementação do sistema Redis Sentinel em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`ansible_host`	Endereço IP da máquina virtual ou servidor físico da seção `nodes` para a implementação do sistema Redis Sentinel. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` • Variável Ansible, por exemplo: `{{ nodes.node_1.ip }}`
`ctl`			Configurações de implementação do controlador. Para implementar uma instância SD-WAN para um locatário, implemente o controlador como uma função de rede física. Em conjunto com cada nó do controlador, o componente MOCKPNF é implementado automaticamente na máquina virtual ou servidor físico para garantir a segurança da configuração do contêiner Docker do nó do controlador.

`tenants`			Configurações de locatários para os quais instâncias SD-WAN estão sendo implementadas.
`- name`			Nome do locatário.
	`state`		Criação de um locatário e implementação do controlador em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
	`ctl_base`		Os primeiros três octetos do endereço IP da rede virtual do controlador. Insira um valor no formato `XXX.XXX.XXX`, por exemplo: `192.168.110` Ao implementar uma plataforma de teste do Kaspersky SD-WAN de acordo com o cenário de implementação tudo-em-um, o valor dessa configuração pode ser o mesmo que o valor da configuração `base` na seção `nodes`.
	`mock_base`		Os três primeiros octetos do endereço IP da rede virtual de gerenciamento do controlador. Insira um valor no formato `XXX.XXX.XXX`, por exemplo: `192.168.110`
	`hosts`		Configurações de implementação do controlador. É possível implementar um nó do controlador sem alta disponibilidade ou três ou cinco nós com alta disponibilidade. Ao implementar três ou cinco nós do controlador, o último se torna o nó de arbitragem.
	`- inventory_hostname`		Nome do host do nó do controlador. Valor padrão: `ctl-<1-5>`.
		`ansible_host`	Endereço IP da máquina virtual ou servidor físico da seção `nodes` para a implementação do nó do controlador. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` • Variável Ansible, por exemplo: `{{ nodes.node_1.ip }}`
	`docker_memory_limit`		Quantidade de RAM, em megabytes, para contêineres Docker do controlador.
	`JAVA_OPTS`		Configurações de RAM da máquina virtual Java.
		`Xms`	A quantidade mínima de memória heap que o Java VM pode alocar ao controlador. Insira um valor em um dos seguintes formatos: • `<quantidade de RAM>m` é a quantidade de RAM em megabytes, por exemplo: `512m` • `<quantidade de RAM>g` é a quantidade de RAM em gigabytes, por exemplo: `2g` Recomendamos especificar um valor com metade do tamanho da configuração `Xmx`.
		`Xmx`	A quantidade máxima de memória heap que o Java VM pode alocar ao controlador. Insira um valor em um dos seguintes formatos: • `<quantidade de RAM>m` é a quantidade de RAM em megabytes, por exemplo: `512m` • `<quantidade de RAM>g` é a quantidade de RAM em gigabytes, por exemplo: `4g` Recomendamos especificar um valor com metade do tamanho da configuração `docker_memory_limit`.
		`MaxDirectMemorySize`	A quantidade máxima de memória direta que o Java VM pode alocar ao controlador. Insira um valor em um dos seguintes formatos: • `<quantidade de RAM>m` é a quantidade de RAM em megabytes, por exemplo: `512m` • `<quantidade de RAM>g` é a quantidade de RAM em gigabytes, por exemplo: `4g` Recomendamos especificar um valor com metade do tamanho da configuração `docker_memory_limit`.

	`syslog_server_address`	Endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviam logs. O valor é especificado no formato `<protocolo>://<endereço do host>:<número da porta>`. Você pode especificar o endereço IP ou FQDN do host como o endereço do host.
		Exemplos:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Se a variável `secure_syslog` estiver definida como `true`, você precisará especificar `tcp+tls` como o prefixo do protocolo, por exemplo:
		`tcp+tls://192.168.2.15:1514`
		Se você quiser usar um coletor KUMA como servidor syslog, especifique o endereço do host no formato FQDN.
		Especifique as configurações do servidor syslog na seção `syslog`.

	`secure_syslog`	Ativa ou desativa a criptografia de mensagens do syslog enviadas pelo contêiner do Docker. Valores possíveis: • `true` • `false` Valor padrão: `false`. Se definido como `false`, as mensagens do syslog são enviadas como texto sem formatação via UDP. Se definido como `true`, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`	O caminho absoluto do arquivo de certificado CA usado para assinar o certificado do servidor syslog. Necessário se `secure_syslog` estiver definido como `true`.
	`syslog_format`	Formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis: `rfc3164` para formato compatível com RFC 3164. `rfc5424` para formato compatível com RFC 5424. `rfc5424micro` para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos. Se você quiser usar um coletor KUMA como servidor syslog, especifique `rfc3164`.
`www`		Configurações da parte de front-end da solução.

`syslog_server_address`		Endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviam logs. O valor é especificado no formato `<protocolo>://<endereço do host>:<número da porta>`. Você pode especificar o endereço IP ou FQDN do host como o endereço do host.
		Exemplos:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Se a variável `secure_syslog` estiver definida como `true`, você precisará especificar `tcp+tls` como o prefixo do protocolo, por exemplo:
		`tcp+tls://192.168.2.15:1514`
		Se você quiser usar um coletor KUMA como servidor syslog, especifique o endereço do host no formato FQDN.
		Especifique as configurações do servidor syslog na seção `syslog`.

`secure_syslog`		Ativa ou desativa a criptografia de mensagens do syslog enviadas pelo contêiner do Docker. Valores possíveis: • `true` • `false` Valor padrão: `false`. Se definido como `false`, as mensagens do syslog são enviadas como texto sem formatação via UDP. Se definido como `true`, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável `syslog_server_ca_cert_file_path`.
`syslog_server_ca_cert_file_path`		O caminho absoluto do arquivo de certificado CA usado para assinar o certificado do servidor syslog. Necessário se `secure_syslog` estiver definido como `true`.
`syslog_format`		Formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis: `rfc3164` para formato compatível com RFC 3164. `rfc5424` para formato compatível com RFC 5424. `rfc5424micro` para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos. Se você quiser usar um coletor KUMA como servidor syslog, especifique `rfc3164`.
`docker_memory_limit`		Quantidade de RAM, em megabytes, para contêineres Docker da parte de front-end da solução.
`oem`		Exibir configurações dos gráficos da interface da Web do orquestrador. Essa seção permite alterar os gráficos da interface da Web do orquestrador.
	`state`	Substituição dos gráficos padrão da interface da Web do orquestrador. Valores possíveis: • `enabled` • `disabled`
	`path_local`	Caminho para o diretório no dispositivo do administrador com os gráficos da interface da Web do orquestrador. Encontre os gráficos padrão da interface da Web do orquestrador no diretório /oem do arquivo de instalação extraído no dispositivo do administrador.
	`path_remote`	Caminho para o diretório em máquinas virtuais ou servidores físicos com os gráficos da interface da Web do orquestrador.
	`title`	Título exibido em segundo plano ao fazer login na interface da Web do orquestrador. Valor padrão: `Kaspersky SD-WAN`. Comprimento recomendado: não mais que 128 caracteres.
	`support`	O endereço da Web exibido na parte inferior da interface da Web do orquestrador. Valor padrão: `support.kaspersky.com`. Comprimento recomendado: não mais que 128 caracteres.
	`assets`	Os gráficos padrão da interface da Web do orquestrador são substituídos pelos colocados nesse diretório no dispositivo do administrador. Valores possíveis: • `enabled` • `disabled` No parâmetro `path_local`, especifique o diretório no dispositivo do administrador que contém os gráficos da interface da Web do orquestrador.

	www_<1-2>		Configurações de implementação de nós da parte de front-end da solução. Você pode implementar um nó da parte de front-end da solução sem alta disponibilidade ou dois nós com alta disponibilidade. Você deve implementar os nós de front-end da solução e os nós do orquestrador nas mesmas máquinas virtuais ou servidores físicos. Por exemplo, implemente o primeiro nó do front-end da solução na mesma máquina virtual ou servidor físico que o primeiro nó do orquestrador. Especifique as configurações do orquestrador na seção `orc`.
		`inventory_hostname`	Nome do host da parte de front-end da solução. Valor padrão: `www-<1-2>`.
		`state`	Implementação da parte de front-end da solução em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`ansible_host`	Endereço IP da máquina virtual ou servidor físico da seção `nodes` para a implementação da parte de front-end da solução. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` • Variável Ansible, por exemplo: `{{ nodes.node_1.ip }}`
`orc`			Configurações do orquestrador.

	`syslog_server_address`	Endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviam logs. O valor é especificado no formato `<protocolo>://<endereço do host>:<número da porta>`. Você pode especificar o endereço IP ou FQDN do host como o endereço do host.
		Exemplos:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Se a variável `secure_syslog` estiver definida como `true`, você precisará especificar `tcp+tls` como o prefixo do protocolo, por exemplo:
		`tcp+tls://192.168.2.15:1514`
		Se você quiser usar um coletor KUMA como servidor syslog, especifique o endereço do host no formato FQDN.
		Especifique as configurações do servidor syslog na seção `syslog`.

	`secure_syslog`	Ativa ou desativa a criptografia de mensagens do syslog enviadas pelo contêiner do Docker. Valores possíveis: • `true` • `false` Valor padrão: `false`. Se definido como `false`, as mensagens do syslog são enviadas como texto sem formatação via UDP. Se definido como `true`, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`	O caminho absoluto do arquivo de certificado CA usado para assinar o certificado do servidor syslog. Necessário se `secure_syslog` estiver definido como `true`.
	`syslog_format`	Formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis: `rfc3164` para formato compatível com RFC 3164. `rfc5424` para formato compatível com RFC 5424. `rfc5424micro` para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos. Se você quiser usar um coletor KUMA como servidor syslog, especifique `rfc3164`.
	`docker_memory_limit`	Quantidade de RAM, em megabytes, para contêineres Docker do orquestrador.
	`JAVA_OPTS`	Configurações de RAM da máquina virtual Java.
	`Xms`	A quantidade mínima de memória heap que o Java VM pode alocar ao orquestrador. Insira um valor em um dos seguintes formatos: • `<quantidade de RAM>m` é a quantidade de RAM em megabytes, por exemplo: `512m` • `<quantidade de RAM>g` é a quantidade de RAM em gigabytes, por exemplo: `4g` Recomendamos especificar um valor com metade do tamanho da configuração `Xmx`.
	`Xmx`	A quantidade máxima de memória heap que a Java VM pode alocar ao orquestrador. Insira um valor em um dos seguintes formatos: • `<quantidade de RAM>m` é a quantidade de RAM em megabytes, por exemplo: `512m` • `<quantidade de RAM>g` é a quantidade de RAM em gigabytes, por exemplo: `4g` Recomendamos especificar um valor com metade do tamanho da configuração `docker_memory_limit`.
	`number_of_containers`	O número de instâncias de contêiner do orquestrador para balanceamento de carga. Intervalo de valores: `1 a 5`. Se essa configuração não for especificada, `1` será usado por padrão. Essa configuração é ignorada se uma matriz de mais de um elemento for especificada no parâmetro `ansible_host` para as seções `orc_1` e `orc_2`.

	orc_<1-2>		Configurações de implementação de nós do orquestrador. É possível implementar um nó do orquestrador sem alta disponibilidade ou dois nós com alta disponibilidade. Os nós do orquestrador e os nós de front-end da solução devem ser implementados nas mesmas máquinas virtuais ou servidores físicos. Por exemplo, implemente o primeiro nó do orquestrador na mesma máquina virtual ou servidor físico que o primeiro nó do front-end da solução. Especifique as configurações do front-end da solução na seção `www`.
		`inventory_hostname`	Nome do host do orquestrador. Valor padrão: `orc-<1-2>`.
		`state`	Implementação do orquestrador em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`ansible_host`	Endereço IP de nós (máquinas virtuais ou servidores físicos) da seção `nodes` para a implementação do orquestrador. É possível especificar um único endereço IP como uma string ou uma lista de endereços IP como uma matriz de strings. O valor do endereço IP pode ser especificado como uma string no formato `XXX.XXX.XXX.XXX` ou como uma variável Ansible. Exemplos: • String no formato `XXX.XXX.XXX.XXX`: `192.168.110.126` • Variável Ansible: `{{ nodes.node_1.ip }}` • Matriz de variáveis Ansible: `{{ [nodes.node_1.ip, nodes.node_2.ip, nodes.node_3.ip, nodes.node_4.ip, nodes.node_5.ip] }}` Se uma matriz for especificada, a configuração `number_of_containers` é ignorada e o balanceamento de carga entre instâncias do orquestrador é obtido migrando os contêineres do orquestrador para nós separados especificados na matriz.
`vnfm`			Configurações do Gerenciador de funções de rede virtual.

syslog_server_address		Endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviam logs. O valor é especificado no formato <protocolo>://<endereço do host>:<número da porta>. Você pode especificar o endereço IP ou FQDN do host como o endereço do host. Exemplos: udp://192.168.2.15:1514 tcp+tls://my-syslog-server:1514 Se a variável secure_syslog estiver definida como true, você precisará especificar tcp+tls como o prefixo do protocolo, por exemplo: tcp+tls://192.168.2.15:1514 Se você quiser usar um coletor KUMA como servidor syslog, especifique o endereço do host no formato FQDN. Especifique as configurações do servidor syslog na seção syslog.
secure_syslog		Ativa ou desativa a criptografia de mensagens do syslog enviadas pelo contêiner do Docker. Valores possíveis: • true • false Valor padrão: false. Se definido como false, as mensagens do syslog são enviadas como texto sem formatação via UDP. Se definido como true, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável syslog_server_ca_cert_file_path.
syslog_server_ca_cert_file_path		O caminho absoluto do arquivo de certificado CA usado para assinar o certificado do servidor syslog. Necessário se secure_syslog estiver definido como true.
syslog_format		Formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis: rfc3164 para formato compatível com RFC 3164. rfc5424 para formato compatível com RFC 5424. rfc5424micro para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos. Se você quiser usar um coletor KUMA como servidor syslog, especifique rfc3164.
docker_memory_limit		Quantidade de RAM, em megabytes, para contêineres Docker do orquestrador.
JAVA_OPTS		Configurações de RAM da máquina virtual Java.
	Xms	A quantidade mínima de memória heap que a Java VM pode alocar ao Gerenciador de funções de rede virtual. Insira um valor em um dos seguintes formatos: • <quantidade de RAM>m é a quantidade de RAM em megabytes, por exemplo: 512m • <quantidade de RAM>g é a quantidade de RAM em gigabytes, por exemplo: 4g Recomendamos especificar um valor com metade do tamanho da configuração Xmx.
	Xmx	A quantidade máxima de memória heap que o Java VM pode alocar ao Gerenciador de funções de rede virtual. Insira um valor em um dos seguintes formatos: • <quantidade de RAM>m é a quantidade de RAM em megabytes, por exemplo: 512m • <quantidade de RAM>g é a quantidade de RAM em gigabytes, por exemplo: 4g Recomendamos especificar um valor com metade do tamanho da configuração docker_memory_limit.
vnfm_<1–2>		Configurações de implementação de nós do Gerenciador de funções de rede virtual. É possível implementar um nó do Gerenciador de funções de rede virtual sem alta disponibilidade ou dois nós com alta disponibilidade.

		`inventory_hostname`	Nome do host do Gerenciador de funções de rede virtual. Valor padrão: `vnfm-<1-2>`.
		`state`	Implementação do Gerenciador de funções de rede virtual em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`ansible_host`	Endereço IP da máquina virtual ou servidor físico da seção `nodes` para a implementação do Gerenciador de funções de rede virtual. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` • Variável Ansible, por exemplo: `{{ nodes.node_1.ip }}`
`vnfm_proxy`			Configurações do Gerenciador de funções de rede virtual proxy.

	`syslog_server_address`		Endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviam logs. O valor é especificado no formato `<protocolo>://<endereço do host>:<número da porta>`. Você pode especificar o endereço IP ou FQDN do host como o endereço do host.
			Exemplos:
			`udp://192.168.2.15:1514`
			`tcp+tls://my-syslog-server:1514`
			Se a variável `secure_syslog` estiver definida como `true`, você precisará especificar `tcp+tls` como o prefixo do protocolo, por exemplo:
			`tcp+tls://192.168.2.15:1514`
			Se você quiser usar um coletor KUMA como servidor syslog, especifique o endereço do host no formato FQDN.
			Especifique as configurações do servidor syslog na seção `syslog`.

	`secure_syslog`		Ativa ou desativa a criptografia de mensagens do syslog enviadas pelo contêiner do Docker. Valores possíveis: • `true` • `false` Valor padrão: `false`. Se definido como `false`, as mensagens do syslog são enviadas como texto sem formatação via UDP. Se definido como `true`, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`		O caminho absoluto do arquivo de certificado CA usado para assinar o certificado do servidor syslog. Necessário se `secure_syslog` estiver definido como `true`.
	`syslog_format`		Formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis: `rfc3164` para formato compatível com RFC 3164. `rfc5424` para formato compatível com RFC 5424. `rfc5424micro` para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos. Se você quiser usar um coletor KUMA como servidor syslog, especifique `rfc3164`.
	`docker_memory_limit`		Quantidade de RAM, em megabytes, para contêineres Docker do Gerenciador de funções de rede virtual proxy.
	`vnfm_proxy_<1-2>`		Configurações de implementação de nós do Gerenciador de funções de rede virtual proxy. É possível implementar um nó do Gerenciador de funções de rede virtual proxy sem alta disponibilidade ou dois nós com alta disponibilidade.
		`inventory_hostname`	Nome do host do Gerenciador de funções de rede virtual proxy. Valor padrão: `vnfm-proxy-<1-2>`.
		`state`	Implementação do Gerenciador de funções de rede virtual proxy em uma máquina virtual ou servidor físico. Valores possíveis: • `enabled` • `disabled`
		`ansible_host`	Endereço IP da máquina virtual ou servidor físico da seção `nodes` para a implementação do Gerenciador de funções de rede virtual proxy. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` • Variável Ansible, por exemplo: `{{ nodes.node_1.ip }}`

Exemplo de arquivo de configuração

```
version: 2.24.03.0
nodes:
 node_1:
 ip: 192.168.2.1
 knaas_aio_int:
 base: 10.11.11
```

```
  mode: bridge
  knaas_os_man:
  base: 10.11.12
  mode: bridge
  node_2:
  ip: 192.168.2.2
  knaas_aio_int:
  base: 10.11.11
  mode: bridge
  knaas_os_man:
  base: 10.11.12
  mode: bridge
  node_3:
  ip: 192.168.2.3
  knaas_aio_int:
  base: 10.11.11
  mode: bridge
  knaas_os_man:
  base: 10.11.12
  mode: bridge
external:
  vault_passwords_dirname: ../passwords
  ansible_user: user
  ssl:
  san_list:
  ip:
  - 192.168.2.4
  dns:
  - sdwan.kaspersky.com
  path_local: ../ssl
  path_remote: /home/user/ssl
  docker:
  local_path_to_images: ../images
  remote_path_to_images: /tmp
  syslog:
  docker_memory_limit: 1024
  max_log_size: 32
  state: enabled
  zabbix:
  syslog_server_address: udp://192.168.2.5:1514
  db_docker_memory_limit: 1024
  srv_docker_memory_limit: 1024
  www_docker_memory_limit: 1024
  proxy_docker_memory_limit: 128
  cachesize: 512M
  zabbix_1:
  ansible_host: {{ nodes.node_1.ip }}
  db:
  inventory_hostname: zabbix-db-1
  state: enabled
  srv:
  inventory_hostname: zabbix-srv-1
  state: enabled
  www:
  inventory_hostname: zabbix-www-1
  state: enabled
  proxy:
  inventory_hostname: zabbix-proxy-1
```

```
state: enabled
zabbix_2:
ansible_host: {{ nodes.node_2.ip }}
db:
inventory_hostname: zabbix-db-2
state: enabled
srv:
inventory_hostname: zabbix-srv-2
state: enabled
www:
inventory_hostname: zabbix-www-2
state: enabled
proxy:
inventory_hostname: zabbix-proxy-2
state: enabled
zabbix_3:
ansible_host: {{ nodes.node_3.ip }}
db:
inventory_hostname: zabbix-db-3
state: enabled
mongo:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 2048
mongo_1:
inventory_hostname: mongo-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
mongo_2:
inventory_hostname: mongo-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
mongo_3:
inventory_hostname: mongo-3
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 4096
redis_1m:
inventory_hostname: redis-1m
state: enabled
ansible_host: {{ nodes.node_1.ip }}
redis_2m:
inventory_hostname: redis-2m
state: enabled
ansible_host: {{ nodes.node_2.ip }}
redis_3m:
inventory_hostname: redis-3m
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis_1s:
inventory_hostname: redis-1s
state: enabled
ansible_host: {{ nodes.node_2.ip }}
redis_2s:
inventory_hostname: redis-2s
state: enabled
ansible_host: {{ nodes.node_3.ip }}
```

```
redis_3s:
inventory_hostname: redis-3s
state: enabled
ansible_host: {{ nodes.node_1.ip }}
ctl:
tenants:
- name: ha3
state: enabled
ctl_base: 10.11.11
mock_base: 10.11.12
hosts:
- inventory_hostname: ctl-1
ansible_host: {{ nodes.node_1.ip }}
- inventory_hostname: ctl-2
ansible_host: {{ nodes.node_2.ip }}
- inventory_hostname: ctl-3
ansible_host: {{ nodes.node_3.ip }}
docker_memory_limit: 8192
JAVA_OPTS:
Xms: 2g
Xmx: 4g
MaxDirectMemorySize: 4g
syslog_server_address: udp://192.168.2.5:1514
www:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
oem:
state: disabled
path_remote: /home/user/oem
path_local: ../../oem
title: OEM Title
support: https://support.support.com
assets: true
www_1:
inventory_hostname: www-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
www_2:
inventory_hostname: www-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
orc:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 4096
JAVA_OPTS:
Xms: 2g
Xmx: 4g
orc_1:
inventory_hostname: orc-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
orc_2:
inventory_hostname: orc-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
vnfm:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
```

```
JAVA_OPTS:
Xms: 512m
Xmx: 1024m
vnfm_1:
inventory_hostname: vnfm-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
vnfm_2:
inventory_hostname: vnfm-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
vnfm_proxy:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
vnfm_proxy_1:
inventory_hostname: vnfm-proxy-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
vnfm_proxy_2:
inventory_hostname: vnfm-proxy-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
inventory_hostname: zabbix-db-2
state: enabled
srv:
inventory_hostname: zabbix-srv-2
state: enabled
www:
inventory_hostname: zabbix-www-2
state: enabled
proxy:
inventory_hostname: zabbix-proxy-2
state: enabled
zabbix_3:
ansible_host: {{ nodes.node_3.ip }}
db:
inventory_hostname: zabbix-db-3
state: enabled
mongo:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 2048
mongo_1:
inventory_hostname: mongo-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
mongo_2:
inventory_hostname: mongo-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
mongo_3:
inventory_hostname: mongo-3
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 4096
redis_1m:
inventory_hostname: redis-1m
```

```
state: enabled
ansible_host: {{ nodes.node_1.ip }}
redis_2m:
inventory_hostname: redis-2m
state: enabled
ansible_host: {{ nodes.node_2.ip }}
redis_3m:
inventory_hostname: redis-3m
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis_1s:
inventory_hostname: redis-1s
state: enabled
ansible_host: {{ nodes.node_2.ip }}
redis_2s:
inventory_hostname: redis-2s
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis_3s:
inventory_hostname: redis-3s
state: enabled
ansible_host: {{ nodes.node_1.ip }}
ctl:
tenants:
- name: ha3
state: enabled
ctl_base: 10.11.11
mock_base: 10.11.12
hosts:
- inventory_hostname: ctl-1
ansible_host: {{ nodes.node_1.ip }}
- inventory_hostname: ctl-2
ansible_host: {{ nodes.node_2.ip }}
- inventory_hostname: ctl-3
ansible_host: {{ nodes.node_3.ip }}
docker_memory_limit: 8192
JAVA_OPTS:
Xms: 2g
Xmx: 4g
MaxDirectMemorySize: 4g
syslog_server_address: udp://192.168.2.5:1514
www:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
oem:
state: disabled
path_remote: /home/user/oem
path_local: ../../oem
title: OEM Title
support: https://support.support.com
assets: true
www_1:
inventory_hostname: www-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
www_2:
inventory_hostname: www-2
state: enabled
```

```
ansible_host: {{ nodes.node_2.ip }}
orc:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 4096
JAVA_OPTS:
Xms: 2g
Xmx: 4g
orc_1:
inventory_hostname: orc-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
orc_2:
inventory_hostname: orc-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
vnfm:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
JAVA_OPTS:
Xms: 512m
Xmx: 1024m
vnfm_1:
inventory_hostname: vnfm-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
vnfm_2:
inventory_hostname: vnfm-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
vnfm_proxy:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
vnfm_proxy_1:
inventory_hostname: vnfm-proxy-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
vnfm_proxy_2:
inventory_hostname: vnfm-proxy-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
```

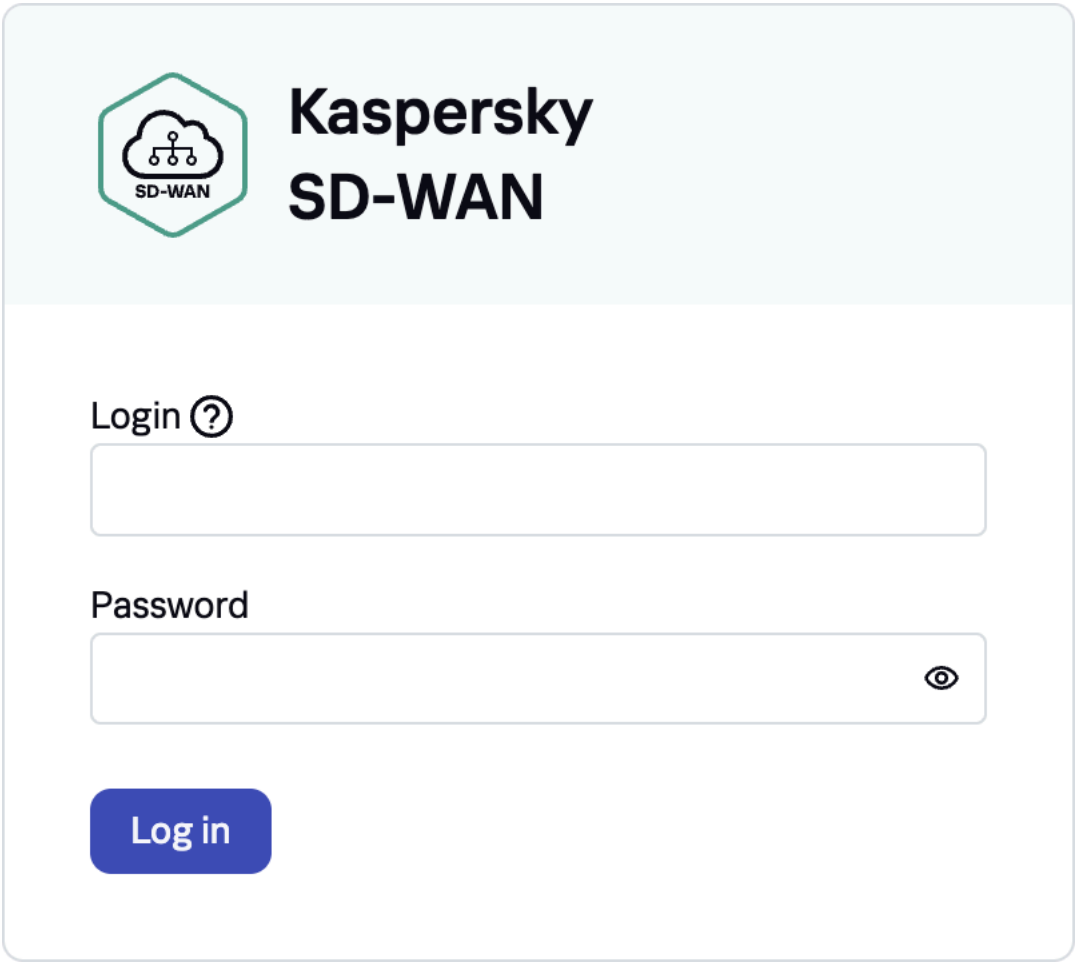
Substituição dos elementos gráficos da interface da Web do orquestrador

Para substituir os gráficos da interface da Web do orquestrador:

1. Configure a parte de front-end da solução na seção `www` do arquivo de configuração.
2. No dispositivo do administrador, acesse o diretório /oem do arquivo de instalação extraído. Este diretório contém os elementos gráficos padrão da interface da Web do orquestrador. Você pode substituir os seguintes arquivos:
   - favicon.png e favicon.svg são o ícone exibido na guia da interface da Web do orquestrador.

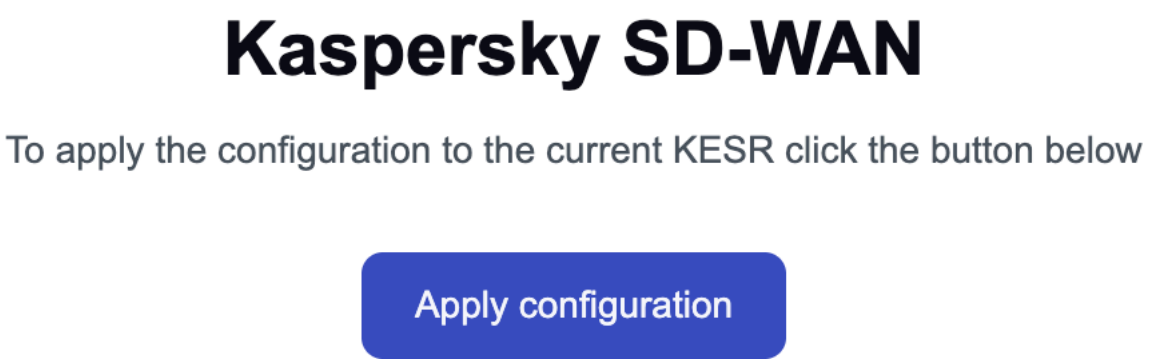
     

   - login_logo.svg é o ícone exibido na parte superior da janela ao fazer login na interface da Web do orquestrador.

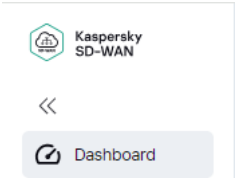
     

- logo_activation.svg é o ícone exibido durante o registro automático de um dispositivo CPE.





- logo.svg e title.svg são o ícone e o título exibidos na parte superior do painel de navegação da interface da Web do orquestrador.



Substituir um nó do controlador com falha

É possível implementar um novo nó do controlador para substituir um que falhou e não pode ser reparado. Se um nó do controlador falhar enquanto estiver em um cluster com outros nós, o novo nó do controlador será automaticamente adicionado a esse cluster e sincronizado com os nós existentes.

Antes de executar esse script, certifique-se de que o endereço IP da máquina virtual ou do servidor físico no qual o novo nó do controlador está sendo implementado seja igual ao endereço IP da máquina virtual ou do servidor físico em que o nó do controlador com falha foi implementado. Os endereços IP das máquinas virtuais ou servidores físicos para implementação de nós do controlador foram especificados ao implementar a solução na seção `ctl` do arquivo de configuração.

O cenário para substituir um nó do controlador com falha envolve as seguintes etapas:

1. **Preparar o dispositivo do administrador**

   Prepare o dispositivo do administrador para implementação do novo nó do controlador. É possível usar uma máquina virtual local ou remota ou um computador pessoal como dispositivo do administrador. Ao implementar uma plataforma de teste do Kaspersky SD-WAN de acordo com o cenário de implementação tudo-em-um, é necessário usar uma máquina virtual como dispositivo do administrador.

2 Garantir a conectividade de rede entre o dispositivo do administrador, os componentes da solução e o novo nó do controlador

Garanta a conectividade de rede entre o dispositivo do administrador, os componentes da solução e a máquina virtual ou o servidor físico em que deseja implementar o novo nó do controlador. Certifique-se de que os links entre máquinas virtuais ou servidores físicos atendam aos requisitos de hardware e software.

> O servidor físico da máquina virtual deve ser implementado em um segmento de rede confiável para evitar comprometer o tráfego transmitido.

3 Implementar um nó do controlador

Faça o seguinte no dispositivo do administrador:

1. Aceite o Contrato de Licença do Usuário Final executando o seguinte comando:

   ```
   export KNAAS_EULA_AGREED="true"
   ```

2. Acesse o diretório com o arquivo de instalação extraído.

3. Para implementar o novo nó do controlador no modo assistido, execute uma das seguintes ações:

   - Caso tenha gerado senhas manualmente durante a implementação da solução, execute o seguinte comando:

     ```
     ansible-playbook -i inventory/generic -e "@< caminho para o arquivo de configuração >" -e "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
     ```

     Ao executar o comando, insira a senha da conta raiz e a senha mestra gerada.

   - Caso não tenha gerado senhas manualmente durante a implementação da solução, execute o seguinte comando:

     ```
     ansible-playbook -i inventory/generic -e "@< caminho para o arquivo de configuração >" -e "@inventory/external/images.yml" -K knaas/knaas-install.yml
     ```

4. Para implementar o novo nó do controlador no modo autônomo, execute uma das seguintes ações:

   > Recomendamos usar esse modo somente em um ambiente confiável, caso contrário, hackers podem interceptar suas senhas.

   - Caso tenha gerado senhas manualmente durante a implementação da solução, execute o seguinte comando:

     ```
     ansible-playbook -i inventory/generic -e "@< caminho para o arquivo de configuração >" -e "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
     ```

   - Caso não tenha gerado senhas manualmente durante a implementação da solução, execute o seguinte comando:

     ```
     ansible-playbook -i inventory/generic -e "@< caminho para o arquivo de configuração >" -e "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" knaas/knaas-install.yml
     ```

O novo nó do controlador é implementado para substituir o nó com falha. Uma mensagem de implementação bem-sucedida é exibida no console do dispositivo do administrador.

Se houver um problema de conectividade de rede com uma máquina virtual ou servidor físico durante a implementação do nó do controlador, um erro será exibido no console do dispositivo do administrador e o novo nó do controlador não será implementado. Nesse caso, restaure a conectividade de rede, limpe a máquina virtual ou o servidor físico e, em seguida, execute o comando de implementação novamente.

Fazer upgrade do Kaspersky SD-WAN

A FUNCIONALIDADE DE ATUALIZAÇÃO (INCLUINDO ATUALIZAÇÕES DE ASSINATURA DE ANTIVÍRUS E ATUALIZAÇÕES DA BASE DE CÓDIGOS), ASSIM COMO A FUNCIONALIDADE DA KSN PODE NÃO ESTAR DISPONÍVEL NO SOFTWARE NO TERRITÓRIO DOS EUA.

Antes de atualizar o Kaspersky SD-WAN, certifique-se de que nenhum dos dispositivos CPE tenha o status **Erro**. Para visualizar o status dos dispositivos CPE, consulte a tabela de dispositivos CPE. Também recomendamos fazer cópias de backup dos componentes da solução:

- Se os componentes da solução estiverem implementados em máquinas virtuais, tire instantâneos das máquinas virtuais. Após atualizar o Kaspersky SD-WAN, é possível excluir os instantâneos das máquinas virtuais. Para obter detalhes sobre como tirar instantâneos de máquinas virtuais, consulte a documentação oficial dos ambientes de virtualização.

- Se os componentes da solução estiverem implementados em servidores físicos, será necessário fazer backups dos discos rígidos dos servidores físicos. Ao usar um controlador RAID (Conjunto Redundante de Discos Independentes), é possível obter informações sobre como criar cópias de backup de seus discos rígidos na documentação oficial do fornecedor do controlador RAID.

O cenário de upgrade do Kaspersky SD-WAN envolve as seguintes etapas:

1. **Preparar o dispositivo do administrador**

   Prepare o dispositivo do administrador para o upgrade da solução. É possível usar uma máquina virtual local ou remota ou um computador pessoal como dispositivo do administrador. Ao implementar uma plataforma de teste do Kaspersky SD-WAN de acordo com o cenário de implementação tudo-em-um, é necessário usar uma máquina virtual como dispositivo do administrador.

2. **Preparar o arquivo de configuração**

   Configure o arquivo de configuração de acordo com as alterações feitas na nova versão do Kaspersky SD-WAN. Veja as alterações no arquivo CHANGELOG.md no diretório raiz do arquivo de instalação.

   Ao fazer o upgrade do Kaspersky SD-WAN, certifique-se de manter os arquivos com senhas e certificados SSL.

3. **Aceitar o Contrato de Licença do Usuário Final**

   Aceite o Contrato de Licença do Usuário Final executando o seguinte comando:

   ```
   export KNAAS_EULA_AGREED="true"
   ```

4. **Fazer upgrade do Kaspersky SD-WAN**

Faça o upgrade do Kaspersky SD-WAN de uma das seguintes formas:

- Para fazer o upgrade da solução no modo assistido:

  ```
  ansible-playbook -i inventory/generic -e "@<caminho para o arquivo de configuração>"
  -e "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
  ```

  Ao executar o comando, insira o senha da conta raiz no dispositivo do administrador e a senha mestra gerada.

- Para fazer o upgrade da solução no modo parcialmente assistido:

  ```
  ansible-playbook -i inventory/generic -e "@<caminho para o arquivo de configuração>"
  -e "@inventory/external/images.yml" -K --vault-password-file
  ./passwords/vault_password.txt knaas/knaas-install.yml
  ```

  Insira a senha raiz do dispositivo do administrador ao executar o comando.

- Para fazer o upgrade da solução no modo autônomo:

  ```
  ansible-playbook -i inventory/generic -e "@<caminho para o arquivo de configuração>"
  -e "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --
  vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
  ```

Os componentes do Kaspersky SD-WAN são atualizado nas máquinas virtuais ou nos servidores físicos especificados no arquivo de configuração. Uma mensagem de upgrade bem-sucedido é exibida no console do dispositivo do administrador.

Em caso de problemas de conexão de rede com uma das máquinas virtuais ou servidores físicos durante o upgrade dos componentes da solução, uma mensagem de erro será exibida no console do dispositivo do administrador e o upgrade da solução não será feito. Nesse caso, será necessário restaurar a conexão de rede e, em seguida, executar o comando de upgrade novamente.

Depois do upgrade da solução, limpe o histórico de comandos do Bash.

Remover o Kaspersky SD-WAN

A remoção do Kaspersky SD-WAN não pode ser revertida.

Para remover o Kaspersky SD-WAN:

1. No dispositivo do administrador, acesse o arquivo de instalação extraído.
2. Remova o Kaspersky SD-WAN de uma das seguintes formas:

   - Para remover a solução no modo assistido:

     ```
     ansible-playbook -i inventory/generic -e "@<caminho para o arquivo de
     configuração>" -e "@inventory/external/images.yml" -K knaas/knaas-teardown.yml
     ```

   - Para remover a solução no modo autônomo:

     ```
     ansible-playbook -i inventory/generic -e "@<caminho para o arquivo de
     configuração>" -e "@inventory/external/images.yml" -e
     "ansible_become_password=yourSudoPassword" knaas/knaas-teardown.yml
     ```

Os componentes do Kaspersky SD-WAN são removidos das máquinas virtuais ou dos servidores físicos. Uma mensagem de remoção bem-sucedida é exibida no console do dispositivo do administrador.

Em caso de problemas de conexão de rede com uma das máquinas virtuais ou servidores físicos durante a remoção dos componentes da solução, uma mensagem de erro será exibida no console do dispositivo do administrador e a remoção da solução não será feita. Nesse caso, será necessário restaurar a conexão de rede e, em seguida, executar o comando de remoção novamente.

Fazer login e logout da interface da Web do orquestrador

Fazer login na interface da Web do orquestrador

Para fazer login na interface da Web do orquestrador:

1. Na barra de endereços do navegador, insira um dos seguintes endereços IP:

   - Para fazer login no portal do administrador, insira o endereço IP da máquina virtual ou do servidor físico no qual implementou o orquestrador ou o front-end da solução. Você especificou o endereço IP da máquina virtual ou do servidor físico para a implementação do orquestrador ou front-end nas seções `orc_<1-2>` e `www_<1-2>` do arquivo de configuração durante a implementação da solução . Também é possível inserir o endereço IP virtual do orquestrador.

   - Para fazer login no portal de autoatendimento, insira o endereço IP fornecido pelo administrador da plataforma.

2. A página de autenticação é aberta; nessa página, insira um nome de usuário e uma senha. A senha deve conter pelo menos uma letra latina maiúscula (A–Z), uma letra minúscula (a–z), um número e um caractere especial. Comprimento da senha: 8 a 50 caracteres.

3. Clique em **Login**. Se a autenticação de dois fatores estiver ativada para sua conta.

   a. Digitalize o código QR exibido com um autenticador físico ou de software compatível com o padrão RFC 6238.

   b. Insira e confirme o código exclusivo gerado pelo autenticador.

Após a autenticação, você será direcionado para a seção ou subseção definida como página padrão.

Fazer login na interface da Web do orquestrador

Para fazer logout da interface da Web do orquestrador:

1. Na parte inferior do menu, clique no ícone de logout .

2. Na janela de confirmação, clique em **OK**.

Você é desconectado da interface da Web do orquestrador.

Licenciamento do Kaspersky SD-WAN

Esta seção aborda os conceitos básicos de licenciamento do Kaspersky SD-WAN. Caso precise dimensionar a solução, adquira licenças adicionais de software e hardware.

Sobre o Contrato de Licença do Usuário Final

O *Contrato de Licença do Usuário Final* é um contrato vinculativo entre você e a AO Kaspersky Lab que estipula os termos nos quais você pode usar o programa. O texto do Contrato de Licença do Usuário Final nos idiomas disponíveis está localizado nos arquivos *de licença <código do idioma>.rtf* incluídos no kit de distribuição do Kaspersky SD-WAN.

Leia com atenção os termos do Contrato de Licença do Usuário Final antes de começar a usar o Kaspersky SD-WAN.

Ao confirmar que concorda com o Contrato de Licença do Usuário Final, você indica a aceitação dos termos do Contrato de Licença do Usuário Final. É possível fazer isso de uma das seguintes maneiras:

- Inicialize a variável de ambiente `KNAAS_EULA_AGREED` antes de iniciar o contêiner Docker do Kaspersky SD-WAN:

  ```
  export KNAAS_EULA_AGREED=yes
  ```

  Nesse caso, ao iniciar o contêiner Docker do Kaspersky SD-WAN, passe a variável de ambiente KNAAS_EULA_AGREED usando a opção `-e`:

  ```
  docker run -e KNAAS_EULA_AGREED [OPTIONS] IMAGE [COMMAND] [ARG...]
  ```

- Inicialize a variável de ambiente `KNAAS_EULA_AGREED` diretamente ao iniciar o contêiner Docker do Kaspersky SD-WAN:

  ```
  docker run -e KNAAS_EULA_AGREED=yes [OPTIONS] IMAGE [COMMAND] [ARG...]
  ```

A variável de ambiente `KNAAS_EULA_AGREED` não é inicializada ou é inicializada com o valor `no` (`KNAAS_EULA_AGREED=no`), o que significa que você não concorda com os termos do Contrato de Licença do Usuário Final. Nesse caso, ao iniciar o contêiner Docker do Kaspersky SD-WAN, uma mensagem de erro é exibida e o Kaspersky SD-WAN não é iniciado.

Sobre a coleta de dados

As seguintes soluções de terceiros estão integradas ao Kaspersky SD-WAN:

- Sistema de monitoramento Zabbix
- Plataforma OpenStack para a criação de serviços e armazenamento na nuvem
- Mapas geográficos do OpenStreetMap

As informações pessoais que podem ser introduzidas no Zabbix, OpenStack ou OpenStreetMap como resultado da integração não são enviadas para fora do perímetro da infraestrutura da organização.

A Kaspersky protege as informações recebidas de acordo com os requisitos estipulados pela lei aplicável e pelas políticas da Kaspersky.

Interface do usuário da solução

O Kaspersky SD-WAN é gerenciado usando a interface da Web do orquestrador. Use as seções do menu para configurar os componentes da solução. Ao navegar até uma seção, um menu adicional com subseções é exibido num formulário recolhido. Para expandir o menu, passe o cursor do mouse sobre o ícone de uma das subseções. Clique no ícone de expansão » para desativar a minimização automática do menu.

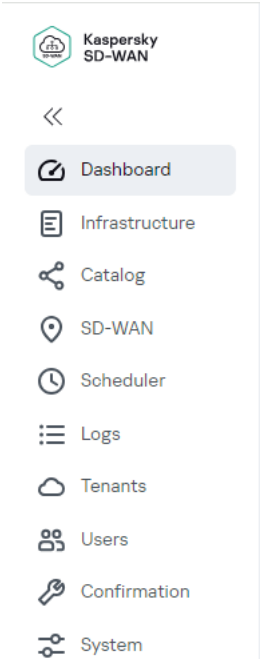
Há suporte para duas variantes da interface da Web do orquestrador:

- O *portal do administrador* dá aos administradores acesso total ao gerenciamento dos componentes da solução.
- O *portal de autoatendimento* dá aos locatários acesso ao gerenciamento das instâncias SD-WAN implementadas para eles.

Os administradores podem fazer login no portal de autoatendimento de um locatário.

Portal do administrador

O menu do portal do administrador é mostrado na figura abaixo.

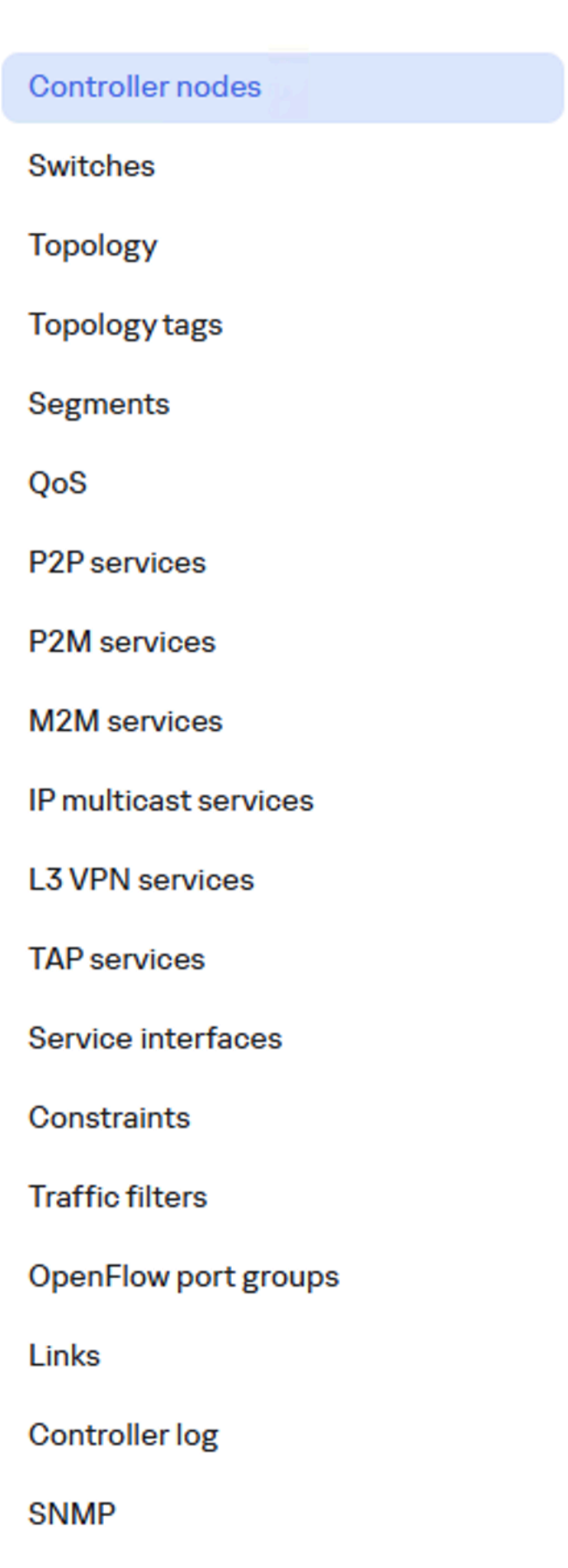


Menu do portal do administrador

Seção	Descrição
Painel	Informações sobre o status atual dos componentes da solução, como dispositivos CPE, funções de rede virtual e funções de rede física.
Infraestrutura	Infraestrutura corporativa. Nesta seção, é possível configurar os seguintes componentes: • Domínios • Data centers • Sub-redes de gerenciamento • Controladores • VIM

Seção	Descrição
Catálogo	Modelos para configuração centralizada de serviços de rede
SD-WAN	• **CPE** — dispositivos CPE para retransmitir o tráfego. • **Modelos de CPE** — modelos de CPE para configuração centralizada de dispositivos CPE. • **Modelos de firewall** — modelos de firewall para configuração centralizada do firewall em dispositivos CPE. • **Zonas de firewall** — zonas de firewall para interfaces de rede e sub-redes de dispositivos CPE. • **Modelos NetFlow** — modelos NetFlow para monitorar informações de pacotes de tráfego em dispositivos CPE. • **Diretórios APN**: lista de diretórios para a configuração automática de APN para interfaces do tipo QMI em dispositivos CPE. • **IPAM** — endereço IP e intervalos de sub-rede para dispositivos CPE. • **Firmware** — firmware do dispositivo CPE. • **Certificados** — certificados de dispositivos CPE. • **Instâncias SD-WAN** — instâncias SD-WAN implementadas. • **Modelos de instância SD-WAN** — modelos para configuração e implementação centralizadas de instâncias SD-WAN. • **Pools de instância SD-WAN** — pools de instâncias SD-WAN. • **Modelos de UNI** — modelos UNI para a criação centralizada de UNIs em dispositivos CPE.
Programador	Tarefas agendadas para serem executadas posteriormente.
Logs	Registros de componentes da solução, como dispositivos CPE, funções de rede virtual e funções de rede física.
Locatários	Locatários da solução.
Usuários	Usuários da solução. Nesta seção, é possível configurar os seguintes componentes: • Usuários • Permissões de acesso • Grupos de usuários LDAP • Conexões LDAP
Confirmação	Solicitações de confirmação para ações do usuário.
Sistema	• **Monitoramento**contém configurações do servidor Zabbix para monitoramento dos componentes da solução. • **Notificação**contém configurações para envio de notificações por e-mail aos usuários. • **Log do orquestrador** é o detalhamento do registro do contêiner Docker. • **Sessões de usuário** contém configurações de sessão do usuário. • **API** é a API do orquestrador. • **Outro** contém configurações adicionais.

O controlador tem seu próprio menu de configuração (veja a figura abaixo). Para informações detalhadas sobre o menu de configuração do controlador, consulte o artigo Visualizar informações sobre nós do controlador.

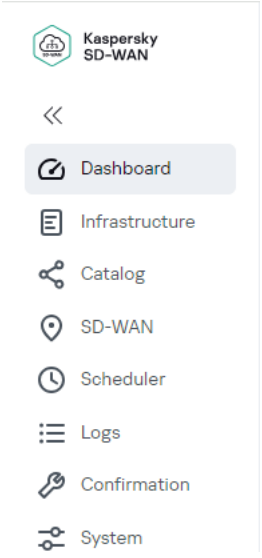


Menu de configuração do controlador no portal do administrador

Seção	Descrição
Nós do controlador	Informações sobre o status atual dos nós do controlador.
Switches	Configurações avançadas de switches e dispositivos CPE.
Topologia	Topologia gráfica de uma instância SD-WAN.
Tags de topologia	Tags de topologia para estabelecer links entre dispositivos CPE.
Segmentos	Segmentos formados a partir de switches e dispositivos CPE.
QoS	Configurações de qualidade de serviço. Nesta seção, é possível configurar os seguintes componentes: • Classes de tráfego • Classificadores de tráfego • Regras de qualidade de serviço
Serviços P2P	Serviços de transporte ponto a ponto.
Serviços P2M	Serviços de transporte ponto a multiponto.
Serviços M2M	Serviços de transporte multiponto a multiponto.
Serviços multicast IP	Serviços de transporte multicast IP.
Serviços de L3 VPN	Serviços de transporte VPN L3.
Serviços TAP	Serviços TAP (Ponto de acesso de teste) para espelhamento de tráfego.
Interfaces de serviço	Interfaces de serviço de switches e dispositivos CPE.
Restrições	Restrições de Manual-TE e restrições de limite para garantia da qualidade do serviço.
Filtros de tráfego	Filtros de tráfego para reforço da qualidade do serviço.
Grupos de portas OpenFlow	Grupos de portas OpenFlow.
Links	Links entre switches e dispositivos CPE e links entre dispositivos CPE.
Logs	Nível de detalhes do log do contêiner Docker.
SNMP	Configurações para monitoramento de dispositivos CPE, funções de rede virtual e funções de rede física usando SNMP.

Portal de autoatendimento

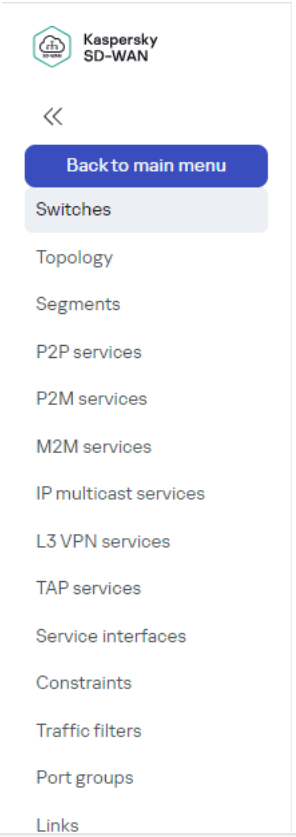
O menu do portal de autoatendimento é mostrado na figura abaixo.



Menu do portal de autoatendimento

Seção	Descrição
Painel	Informações sobre o status atual dos componentes da solução, como dispositivos CPE e funções de rede.
Infraestrutura	Infraestrutura corporativa. Nesta seção, é possível configurar os controladores.
Catálogo	Serviços de rede para transmissão de tráfego e virtualização de funções de rede.
SD-WAN	• **CPE** — dispositivos CPE para retransmitir o tráfego. • **Modelos de CPE** — modelos de CPE para configuração centralizada de dispositivos CPE. • **Modelos de firewall** — modelos de firewall para configuração centralizada do firewall em dispositivos CPE. • **Zonas de firewall** — zonas de firewall para interfaces de rede e sub-redes de dispositivos CPE. • **Modelos NetFlow** — modelos NetFlow para monitorar informações de pacotes de tráfego em dispositivos CPE. • **IPAM** — endereço IP e intervalos de sub-rede para dispositivos CPE. • **Modelos de UNI** — modelos UNI para a criação centralizada de UNIs em dispositivos CPE.
Programador	Tarefas agendadas para serem executadas posteriormente.
Logs	Registros de componentes da solução, como dispositivos CPE, funções de rede virtual e funções de rede física.
Confirmação	Solicitações de confirmação para ações do usuário.
Sistema	• **Notificação**contém configurações para envio de notificações por e-mail aos usuários. • **Sessões de usuário** contém configurações de sessão do usuário.

O controlador tem seu próprio menu de configuração (veja a figura abaixo).



Seção	Descrição
Switches	Configurações avançadas de switches e dispositivos CPE.
Topologia	Topologia gráfica de uma instância SD-WAN.
Segmentos	Segmentos formados a partir de switches e dispositivos CPE.
Serviços P2P	Serviços de transporte ponto a ponto.
Serviços P2M	Serviços de transporte ponto a multiponto.
Serviços M2M	Serviços de transporte multiponto a multiponto.
Serviços multicast IP	Serviços de transporte multicast IP.
Serviços de L3 VPN	Serviços de transporte VPN L3.
Serviços TAP	Serviços TAP para espelhamento de tráfego.

Seção	Descrição
Interfaces de serviço	Interfaces de serviço de switches e dispositivos CPE.
Restrições	Restrições de Manual-TE e restrições de limite para garantia da qualidade do serviço.
Filtros de tráfego	Filtros de tráfego para reforço da qualidade do serviço.
Grupos de portas OpenFlow	Grupos de portas OpenFlow.
Links	Links entre switches e dispositivos CPE e links entre dispositivos CPE.

Configurar e redefinir a página padrão

A página padrão é uma seção ou subseção do menu exibida automaticamente após o login na interface da Web do orquestrador.

Para definir ou redefinir a página padrão:

1. Vá para a seção ou subseção da interface da Web do orquestrador que deseja definir como página padrão.
2. Abra o menu de configurações da interface da Web no canto superior direito da página.
3. No menu, selecione Página padrão →Definir como página padrão.

   Na parte superior da página, é exibida a mensagem A página padrão foi definida.
4. Se você quiser redefinir a página padrão, selecione **Página padrão →Redefinir página padrão**.

   Na parte superior da página, é exibida a mensagem *A página padrão foi redefinida*. A seção Painel se torna a página padrão.

Alternar entre os modos claro e escuro da interface da Web do orquestrador

Para alternar entre os modos claro e escuro da interface da Web do orquestrador:

1. Abra o menu de configurações da interface da Web no canto superior direito da página.
2. No menu, ative ou desative o interruptor de alternância Modo escuro.

Alterar o idioma da interface da Web do orquestrador

A interface da Web do orquestrador é compatível com os seguintes idiomas:

- English
- Russo

- Espanhol (México)
- Português (Brasil)

Para alterar o idioma da interface da Web do orquestrador:

1. Abra o menu de configurações da interface da Web no canto superior direito da página.
2. No menu, selecione o item com o símbolo de globo e o nome do idioma da interface atual e, em seguida, selecione um idioma na lista suspensa.

Gerenciar tabelas de componentes da solução

Os componentes da solução, como usuários, interfaces de rede e pares BGP são exibidos em tabelas. Use os seguintes controles para gerenciar as tabelas:

- O ícone de configurações, que pode ser usado para:
  - Atualizar a tabela clicando no ícone de configurações →**Recarregar**. Também é possível atualizar a tabela usando o ícone de atualização.
  - Restaurar as larguras padrão das colunas da tabela clicando no ícone de configurações → **Redefinir largura das colunas**.
  - Selecione quais colunas são exibidas na tabela. Para isso, clique no ícone de configurações e marque as caixas de seleção ao lado das colunas que deseja exibir.
- O ícone de pesquisa para clicar e inserir critérios de pesquisa. Após inserir os critérios de pesquisa, a tabela exibe as entradas relevantes.
- Filtros de status para exibir entradas com o status selecionado.
- Filtros de tempo para exibir entradas para o período selecionado:
  - **Todo o tempo**
  - **Último ano**
  - **Último mês**
  - **Última semana**
  - **Último dia**

  É possível especificar o período manualmente usando os campos na parte superior da tabela.
- O botão **Ações** para aplicar uma ação simultaneamente em todas as entradas com caixas de seleção marcadas. Por exemplo, na tabela de dispositivos CPE, é possível excluir vários dispositivos CPE ao mesmo tempo.

A largura de cada coluna da tabela pode ser ajustada usando os ícones de três pontos entre os nomes das colunas.

Navegar até a API do orquestrador

Para navegar até a API do orquestrador:

1. No menu, acesse a seção **Sistema**.

   Por padrão, é selecionada a guia **Monitoramento**, que exibe as configurações de conexão do servidor Zabbix.

2. Selecione a guia **API**.

Isso abre uma lista de comandos da API que podem ser usados para gerenciar o orquestrador.

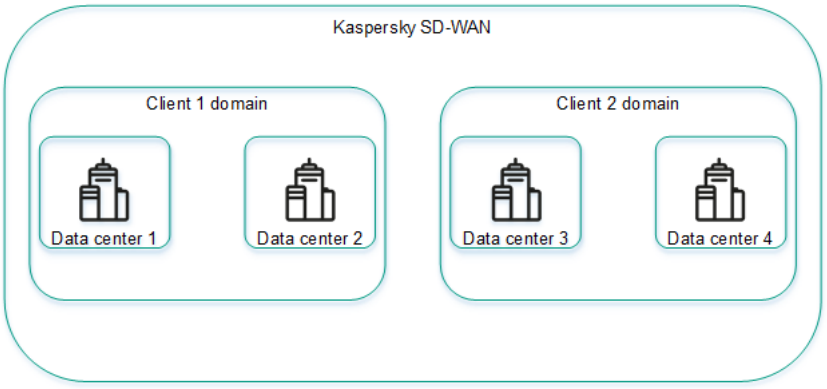
Gerenciar a infraestrutura do Kaspersky SD-WAN

Os locais onde são implementados todos os componentes do Kaspersky SD-WAN que não sejam dispositivos CPE se chamam *data centers*. É necessário adicionar os data centers à interface da Web do orquestrador para gerenciar os controladores e VIMs, além de especificar o servidor proxy Zabbix para configurar o monitoramento dos componentes da solução.

Caso haja muitos data centers, é possível adicioná-los a domínios. *Domínios* são agrupamentos lógicos de data centers com base em um determinado critério, como localização geográfica. Antes de adicionar data centers, crie pelo menos um domínio. É possível mover data centers entre domínios.

Em cada data center, crie pelo menos uma sub-rede de gerenciamento para atribuir endereços IP, servidores DNS e rotas estáticas a dispositivos CPE e funções de rede virtual.

A figura abaixo mostra o diagrama de uma organização. Os componentes do Kaspersky SD-WAN estão implementados em quatro data centers. A organização fornece a solução para dois clientes, cada um com uma instância SD-WAN implementada. Dois data centers são usados para implementar cada instância SD-WAN. Os data centers são adicionados aos domínios que correspondem aos clientes.



Exemplo de uma organização com domínios e data centers

Gerenciar domínios

A lista de domínios pode ser visualizada na seção **Infraestrutura**, no painel **Recursos**. Abaixo dos domínios, a lista exibe os data centers adicionados a eles.

Criar um domínio

Para criar um domínio:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Na parte superior da página, clique em **+ Domínio**.

3. Na janela aberta, no campo **Nome**, insira o nome do domínio. O comprimento máximo do nome é de 50 caracteres.

4. Se necessário, no campo **Descrição**, insira uma breve descrição do domínio. O comprimento máximo da descrição é de 100 caracteres.

5. Clique em **Criar**.

   O domínio é criado e exibido no painel **Recursos**.

É possível adicionar data centers a um domínio ao adicionar data centers.

Editar um domínio

Para editar um domínio:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. No painel **Recursos**, clique no ícone de configurações → **Editar** ao lado do domínio que deseja editar.

3. Na janela aberta, se necessário, edite o nome e/ou a descrição do domínio.

4. Clique em **Salvar**.

   O domínio é modificado e exibido no painel **Recursos**.

Excluir um domínio

Antes de excluir um domínio, é necessário excluir os data centers adicionados ao domínio.

Domínios excluídos não podem ser restaurados.

Para excluir um domínio:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. No painel **Recursos**, clique no ícone de configurações → **Excluir** ao lado do domínio que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   O domínio é excluído e não é mais exibido no painel **Recursos**.

Gerenciar data centers

As listas de data centers são exibidas na **Infraestrutura**, no painel **Recursos**, em domínios. Antes de adicionar data centers, crie pelo menos um domínio.

Adicionar um data center

Para adicionar um data center:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Na parte superior da página, clique em **+ Data center**.

3. Na janela aberta, no campo **Nome**, insira o nome do data center. O comprimento máximo do nome é de 50 caracteres.

4. Se necessário, no campo **Descrição**, insira uma breve descrição do data center. O comprimento máximo da descrição é de 100 caracteres.

5. Na lista suspensa **Domínio**, selecione o domínio criado ao qual deseja adicionar o data center. Após adicionar o data center, é possível migrá-lo para outro domínio.

6. Para implementar funções de rede virtual e executar scripts em dispositivos CPE, no campo **URL do VNFM**, insira o endereço da Web do gerenciador de funções de rede virtual ao qual o orquestrador se conecta. Para verificar se o VNFM está disponível, clique em **Testar conexão**.

7. Se necessário, no campo **Localização**, insira o endereço geográfico do data center.

8. Clique em **Criar**.

O data center é adicionado e exibido no painel **Recursos**.

Editar um data center

Para editar um data center:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. No painel **Recursos**, clique no ícone de configurações ⚙ → **Editar** ao lado do data center que deseja editar.

3. Na janela aberta, se necessário, edite as seguintes configurações:
   - Nome do data center
   - Breve descrição do data center
   - URL do Gerenciador de funções de rede virtual
   - Endereço do data center
4. Clique em **Salvar**.

O data center é modificado e atualizado no painel **Recursos**.

Migrar um data center para um domínio diferente

Para migrar um data center para um domínio diferente:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.
2. No painel **Recursos**, clique no ícone de configurações → **Migrar** ao lado do data center que deseja migrar para um domínio diferente.
3. Na janela aberta, selecione o domínio criado para o qual deseja migrar o data center.
4. Clique em **Migrar**.

O data center é migrado para o novo domínio e exibido sob o novo domínio no painel **Recursos**.

Excluir um data center

A exclusão de um data center impossibilita o gerenciamento de controladores, VIMs e sub-redes de gerenciamento no data center. Também não permite especificar o servidor proxy Zabbix para configurar o monitoramento do componente da solução.

Data centers excluídos não podem ser restaurados.

Para excluir um data center:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.
2. No painel **Recursos**, clique no ícone de configurações → **Excluir** ao lado do data center que deseja excluir.
3. Na janela de confirmação, clique em **Excluir**.

O data center é excluído e não é mais exibido no painel **Recursos**.

Gerenciar sub-redes de gerenciamento

Para visualizar a tabela de sub-redes de gerenciamento, vá para a seção **Infraestrutura** do menu, clique no data center adicionado e selecione a guia **IPAM**. As informações sobre sub-redes de gerenciamento são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da sub-rede de gerenciamento.
- **Tipo** é o tipo da sub-rede. No momento, só há suporte para sub-redes de gerenciamento.
- **CIDR** é o prefixo IPv4 da sub-rede de gerenciamento.
- **Gateway** são endereços IPv4 de gateways que a sub-rede de gerenciamento atribui às funções de rede virtual.
- **Intervalo de IPs** são intervalos de endereços IP a partir dos quais a sub-rede de gerenciamento atribui endereços IP a dispositivos CPE e funções de rede virtual.
- **DNS** são endereços IPv4 dos servidores DNS que a sub-rede de gerenciamento atribui às funções de rede virtual.
- **Rotas estáticas** são endereços IPv4 de origem e destino de rotas estáticas que a sub-rede de gerenciamento atribui às funções de rede virtual.
- **Utilização** é o número de endereços IP que a sub-rede de gerenciamento atribuiu a dispositivos CPE e funções de rede virtual.

É possível ver uma tabela de dispositivos CPE e funções de rede virtual aos quais a sub-rede de gerenciamento atribuiu endereços IP. Para isso, selecione a guia **Utilização**. As informações sobre dispositivos CPE e funções de rede virtual são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da sub-rede de gerenciamento que atribuiu um endereço IP ao CPE ou à função de rede virtual.
- **Endereço IP** é o endereço IP atribuído ao dispositivo CPE ou à função de rede virtual.
- **Nome do cliente** é o nome do dispositivo CPE ou da função de rede virtual.
- **Tipo de cliente** são informações sobre se a sub-rede de controle atribuiu um endereço IP ao dispositivo CPE ou à função de rede virtual:
  - **VNF**
  - **CPE**
- **Locatário**é o locatário ao qual o dispositivo CPE foi adicionado ou a função de rede virtual foi atribuída.

As ações que podem ser executadas com as tabelas são descritas nas instruções Gerenciar tabelas de componentes da solução.

Criar uma sub-rede de gerenciamento

Para criar uma sub-rede de gerenciamento:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. No painel **Recursos**, selecione o domínio criado e, em seguida, selecione o data center adicionado no qual deseja criar a sub-rede de gerenciamento. Depois que a sub-rede de gerenciamento é criada, ela não pode ser movida para um data center diferente.

3. Selecione a guia **IPAM**.

   Por padrão, é selecionada a guia **Sub-rede**, que exibe a tabela de sub-redes de gerenciamento.

4. Na parte superior da página, clique em **+ Sub-rede**.

5. No campo **Nome**, insira o nome da sub-rede de gerenciamento.

6. Na lista suspensa **Versão de IP**, selecione a versão dos endereços IP na sub-rede de gerenciamento:

   - **IPv4**. Essa é a configuração padrão.
   - **IPv6**.

7. No campo **CIDR**, insira o prefixo IPv4 da sub-rede de gerenciamento.

8. Caso deseje que a sub-rede de gerenciamento atribua um gateway específico às funções de rede virtual, insira o endereço IPv4 do gateway no campo **Gateway**.

9. Especifique o intervalo de endereços IP a partir dos quais a sub-rede de gerenciamento atribui endereços IP a dispositivos CPE e funções de rede virtual. Para isso, em **Intervalo de IPs**, clique em **+ Adicionar** e nos campos exibidos, insira os valores inicial e final do intervalo de endereços IP.

   O intervalo de endereços IP é especificado e exibido na seção **Intervalo de IPs**. É possível especificar diversos intervalos de endereços IP ou excluir intervalos de endereços IP. Para excluir um intervalo de endereços IP, clique no ícone de exclusão ✕ ao lado dele.

10. Especifique o servidor DNS que a sub-rede de gerenciamento atribui às funções de rede virtual. Para isso, em **DNS**, clique em **+ Adicionar** e, no campo exibido, insira o endereço IPv4 do servidor DNS.

    O servidor DNS é especificado e exibido na seção **DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique no ícone de exclusão ✕ ao lado dele.

11. Especifique a rota estática que a sub-rede de gerenciamento atribui às funções de rede virtual. Para isso, em **Rotas estáticas**, clique em **+ Adicionar** e, nos campos exibidos, insira os endereços IPv4 de origem e destino da rota estática.

    A rota estática é especificada e exibida na seção **Rotas estáticas**. É possível especificar várias rotas estáticas ou excluir rotas estáticas. Para excluir uma rota estática, clique no ícone de exclusão ✕ ao lado dela.

12. Clique em **Criar**.

A sub-rede de gerenciamento é criada e exibida na tabela.

Editar uma sub-rede de gerenciamento

Para editar uma sub-rede de gerenciamento:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. No painel **Recursos**, selecione o domínio criado e, em seguida, o data center adicionado em que a sub-rede de gerenciamento foi criada.

3. Selecione a guia **IPAM**.

   Por padrão, é selecionada a guia **Sub-rede**, que exibe a tabela de sub-redes de gerenciamento.

4. Clique em **Gerenciamento** → **Editar** ao lado da sub-rede de gerenciamento que deseja editar.

5. Na janela aberta, se necessário, edite as seguintes configurações:

   - Nome da sub-rede de gerenciamento
   - Prefixo IPv4 da sub-rede de gerenciamento
   - Endereços IPv4 de gateways que a sub-rede de gerenciamento atribui às funções de rede virtual
   - Intervalos de endereços IP a partir dos quais a sub-rede de gerenciamento atribui endereços IP a dispositivos CPE e funções de rede virtual
   - Servidores DNS que a sub-rede de gerenciamento atribui às funções de rede virtual
   - Rotas estáticas que a sub-rede de gerenciamento atribui às funções de rede virtual

6. Clique em **Salvar**.

A sub-rede de gerenciamento é modificada e atualizada na tabela.

Excluir uma sub-rede de gerenciamento

Sub-redes de gerenciamento excluídas não podem ser restauradas.

Para excluir uma sub-rede de gerenciamento:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. No painel **Recursos**, selecione o domínio criado e, em seguida, o data center adicionado em que a sub-rede de gerenciamento foi criada.

3. Selecione a guia **IPAM**.

   Por padrão, é selecionada a guia **Sub-rede**, que exibe a tabela de sub-redes de gerenciamento.

4. Clique em **Gerenciamento** → **Excluir** ao lado da sub-rede de gerenciamento que deseja excluir.

5. Na janela de confirmação, clique em **Excluir**.

A sub-rede de gerenciamento é excluída e não é mais exibida na tabela.

Gerenciar controladores

Para visualizar a tabela de controladores, vá para a seção **Infraestrutura** do menu, clique no data center criado e selecione a guia **Recursos de rede**. As informações sobre controladores são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do controlador.
- **Estratégias de serviços/transporte** é a estratégia de transporte sendo usada.
- **Tipo de conexão** é o tipo de conexão dos dispositivos CPE ao controlador:
  - **Unicast**
  - **Multicast**
- **Status do cluster** é o status do cluster de nós do controlador:
  - **Para cima** significa que o cluster está operando normalmente.
  - **Degradado** significa que ocorreu um erro durante a operação do cluster.
  - **Para baixo** significa que o cluster não está operacional.
- **Nós do controlador** são endereços IP de nós do controlador.
- **Status do nó** é o status dos nós do controlador:
  - **Conectado** significa que o nó está conectado ao controlador.
  - **Desconectado** significa que o nó não está conectado ao controlador.
  - **Indisponível** significa que o nó não está disponível.
  - **Desconhecido** significa que o status do nó é desconhecido.
- **Função no cluster** é a função do nó no cluster:
  - **Principal** significa que o nó está conectado ao controlador e é o nó principal do cluster.
  - **Secundário** significa que o nó está conectado ao controlador e é um nó secundário no cluster.
  - **Único** significa que o nó está conectado ao controlador e é o único nó no cluster.

- **Árbitro** significa que o nó é o árbitro.
- **Conectado (transição)** significa que a função do nó no cluster está sendo alterada.
- **Não está em um cluster** significa que o nó não foi adicionado a um cluster.
- **Indisponível** significa que o nó não está disponível.
- **Desconhecido** significa que o status do nó é desconhecido.

- **Nó de leitura gRPC ativo** indica se o nó está selecionado como nó prioritário para operações de leitura para fins de balanceamento de carga.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Editar um controlador

Para editar um controlador:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Editar** ao lado do controlador que deseja editar.
3. Na janela aberta, no campo **Nome**, insira o nome do controlador. Intervalo de valores: 1 a 128 caracteres.
4. Se necessário, no campo **Descrição**, insira uma breve descrição do controlador.
5. No campo **Instalação do controlador em servidores <1>/<3>/<5>**, selecione o número de nós do controlador.
6. Na lista suspensa **Tipo de conexão**, selecione o tipo de conexão dos dispositivos CPE ao controlador:
   - **Unicast**
   - **Multicast**
7. Configure o nó do controlador:
   a. No campo **Endereço IP ou nome do host**, insira o endereço IP ou nome do host do nó do controlador.
   b. No campo **Porta gRPC**, insira o número da porta gRPC do nó do controlador.
   c. No campo **Porta JGroups**, insira o número da porta jGroups do nó do controlador.
   d. Para tornar o nó do controlador o nó principal, selecione a opção **Principal**.

   É possível configurar vários nós do controlador.

8. Para alterar como a carga é distribuída entre os nós no cluster do controlador ao ler dados, na lista suspensa **Modo de balanceamento de carga de leitura de gRPC**, selecione um modo de balanceamento:

   - **Apenas nó principal**.

     As operações de leitura são executadas exclusivamente através do nó de cluster principal.

   - **Priorizar nó secundário aleatório**.

     As operações de leitura são executadas com a prioridade dada a um nó de cluster secundário escolhido aleatoriamente.

   - **Selecionar manualmente**.

     As operações de leitura são executadas por meio de um nó de cluster priorizado explicitamente especificado.

   Ao selecionar o modo **Selecionar manualmente**, na lista **Nó selecionado** exibida, selecione o nó prioritário através do qual deseja que as operações de leitura sejam executadas.

9. Clique em **Salvar**.

O controlador é modificado e atualizado na tabela.

Reprovisionar um controlador

Durante o reprovisionamento, as propriedades do controlador são redefinidas para os valores padrão. Isso pode ajudar a resolver erros.

Para reprovisionar o controlador:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Reaprovisionamento** ao lado do controlador que deseja reprovisionar.

3. Na janela de confirmação, clique em **Reaprovisionamento**.

O controlador é reprovisionado.

Restaurar as configurações do controlador

É possível baixar um arquivo com as configurações do controlador especificadas no menu de configuração do controlador. Por exemplo, esse arquivo contém configurações de serviços de transporte e de qualidade de serviço. Se necessário, é possível restaurar as configurações do controlador usando o arquivo baixado.

Para restaurar as configurações do controlador:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Baixar arquivo de backup** ao lado do controlador cujo arquivo de configurações deseja baixar.

   Um arquivo com as configurações do controlador no formato YAML é salvo no dispositivo local.

3. Clique em **Gerenciamento**→ **Restaurar** ao lado do controlador cujas configurações deseja restaurar.

4. Na janela aberta, especifique o caminho para o arquivo baixado com as configurações do controlador.

5. Clique em **Restaurar**.

O controlador é restaurado com as configurações do arquivo de configurações do controlador.

Ativar ou desativar o modo de manutenção em um controlador

É possível ativar o modo de manutenção no controlador ao executar o trabalho de manutenção relacionado à rede SD-WAN para minimizar o impacto do controlador em partes da rede SD-WAN que não são afetadas pelo trabalho de manutenção. No modo de manutenção, o controlador monitora o status da rede SD-WAN, mas não executa nenhuma ação quando os parâmetros da rede SD-WAN são alterados. Por exemplo, no modo de manutenção, o controlador não reconstrói links e caminhos, não reescreve endereços MAC de interfaces de serviço nem altera os serviços de transporte.

Ao desativar o modo de manutenção, o controlador executa ações correspondentes às alterações feitas nos parâmetros da rede SD-WAN.

Para ativar ou desativar o modo de manutenção no controlador:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Execute um dos seguintes:

   - Para ativar o modo de manutenção no controlador, clique em **Gerenciamento**→ **Ativar manutenção** ao lado dele.
   - Para desativar o modo de manutenção no controlador, clique em **Gerenciamento**→ **Desativar manutenção** ao lado dele.

O modo de manutenção é ativado ou desativado no controlador.

Excluir um controlador

Os controladores excluídos não podem ser restaurados.

Para excluir um controlador:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Excluir** ao lado do controlador que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

O controlador é excluído e não é mais exibido na tabela.

Gerenciar as propriedades do controlador

As propriedades regulam a operação do controlador. Cada propriedade tem um *método de alteração* que determina se o valor da propriedade pode ser alterado e quando a alteração entra em vigor. Os seguintes métodos de alteração estão disponíveis:

- **Somente leitura** significa que a propriedade não pode ser alterada.
- **Recarregar** significa que ao alterar uma propriedade, o orquestrador confirma o novo valor no banco de dados do controlador. O novo valor entra em vigor depois que o controlador é reiniciado.

  Um valor de propriedade que está no banco de dados, mas ainda não entrou em vigor é chamado de *valor planejado*. Exclua o valor planejado antes de reiniciar o controlador para manter o valor atual.
- **Tempo de execução** significa que o novo valor entra em vigor imediatamente quando a propriedade é modificada.

A modificação das propriedades pode levar à operação instável do controlador, portanto, recomendamos entrar em contato com o Suporte Técnico da Kaspersky antes de gerenciar as propriedades.

É possível visualizar a tabela de todas as propriedades do controlador ou somente propriedades modificáveis:

- Para visualizar a tabela de todas as propriedades do controlador, vá para a seção **Infraestrutura**, clique no data center adicionado, selecione a guia **Recursos de rede** e clique em**Gerenciamento** → **Propriedades** ao lado do controlador.
- Para visualizar a tabela de propriedades modificáveis do controlador, vá para a seção **Infraestrutura**, clique no data center adicionado, selecione a guia **Recursos de rede**, clique em **Gerenciamento** → **Propriedades**ao lado do controlador e selecione a guia **Propriedades alteráveis**.

As informações sobre propriedades do controlador são exibidas nas seguintes colunas da tabela:

- **Alterar método** é o método de alteração da propriedade.
- **Propriedade** é o nome da propriedade.
- **Valor atual** é o valor atual da propriedade.
- **Valor planejado** é o valor planejado da propriedade. Essa coluna é exibida apenas na guia **Propriedades alteráveis**.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Descrição das propriedades editáveis do controlador

A modificação das propriedades pode levar à operação instável do controlador, portanto, recomendamos entrar em contato com o Suporte Técnico da Kaspersky antes de gerenciar as propriedades.

Propriedade	Descrição
`controller.buffers.in`	Tamanho do buffer, em bytes, para mensagens provenientes de switches no controlador.
`controller.buffers.out`	Tamanho do buffer, em bytes, para mensagens enviadas para switches no controlador.
`controller.listen.port`	O número da porta inicial no intervalo de portas do switch. Portas com os próximos três números consecutivos são adicionadas ao intervalo. Por exemplo, ao inserir `6553`, o intervalo de portas do switch incluirá as portas 6553, 6554, 6555, 6556.
`controller.sockets.config.nodelay`	Se o parâmetro `TCP_NODELAY` é usado para sessões de gerenciamento entre os switches e o controlador. Valores possíveis: • `true` • `false`
`controller.sockets.mode.epoll`	Se o sistema epoll é usado pelo controlador ao gerenciar switches. Valores possíveis: • `true` • `false`
`controller.sockets.timeouts.idle.both`	Tempo, em milissegundos, após o qual as sessões de gerenciamento entre os switches e o controlador ficam ociosas na ausência de operações de leitura ou gravação. A contagem reinicia sempre que uma operação de leitura ou gravação é executada.
`controller.sockets.timeouts.idle.read`	Tempo, em milissegundos, após o qual as sessões de gerenciamento entre os switches e o controlador ficam ociosas na ausência de operações de leitura. A contagem reinicia sempre que uma operação de leitura é executada.
`controller.sockets.timeouts.idle.write`	Tempo, em milissegundos, após o qual as sessões de gerenciamento entre os switches e o controlador ficam ociosas na ausência de operações de gravação. A contagem reinicia sempre que uma operação de gravação é executada.
`controller.threads.affinity`	Os threads Netty são executados preferencialmente em núcleos de CPU separados para switches separados. Valores possíveis: • `true` • `false`
`controller.threads.boss`	Número de threads Netty para lidar com novas conexões de switch.
`controller.tls.ca.certificate.path`	Caminho para o arquivo PEM do certificado raiz usado para assinar o certificado OpenFlow.
`controller.tls.certificate.path`	Caminho para o arquivo PEM do certificado de criptografia para tráfego OpenFlow entre o controlador e os switches.
`controller.tls.private.key.path`	Caminho para o arquivo PEM com a chave privada do certificado OpenFlow.
`controller.watermark.high`	Quando o buffer Netty da sessão de gerenciamento entre os switches e o controlador contém esse número de bytes, a fila é usada para gravar na sessão.
`controller.watermark.low`	Quando o buffer Netty da sessão de gerenciamento entre os switches e o controlador contém esse número de bytes, a fila não é mais usada para gravar na sessão. Essa propriedade é usada quando o número de bytes atinge o valor `controller.watermark.high`.

Propriedade	Descrição
`core.catcher.meter.value.kbits`	A taxa de transferência do vigilante nos switches ao enviar pacotes de tráfego através da sessão de gerenciamento entre os switches e o controlador. Os pacotes de tráfego são copiados por regras de fluxo de interceptação.
`core.drop.rule.idle.sec`	Tempo, em segundos, após o qual as regras de fluxo criadas automaticamente pelo controlador ao processar o primeiro pacote de tráfego interceptado são excluídas nos switches para bloquear pacotes subsequentes. A contagem é reiniciada sempre que a regra de fluxo é aplicada.
`core.link.bonding.enable`	Ligação de links paralelos entre dois switches. Valores possíveis: • `true` • `false`
`core.link.bonding.equal.cost`	Se o algoritmo de custo igual é usado ao vincular links. Valores possíveis: • `true` • `false` Ao especificar `false`, o algoritmo de custo desigual será usado.
`core.link.bonding.max.links`	Número máximo de links em um link vinculado.
`core.link.bonding.mode`	Tipo do grupo de links vinculados. Valores possíveis: • `BALANCING` significa que o tráfego é balanceado entre links de acordo com um valor de hash. O hash é calculado com base nos campos `IP Proto`, `IP src-dst` e `Port src-dst` dos pacotes de tráfego. • `BROADCAST` significa que o tráfego é duplicado por meio de todos os links.
`core.link.check.ports.status`	Se o controlador envia periodicamente pacotes LLDP apenas para portas ativadas para detectar links entre switches. Valores possíveis: • `true` • `false`
`core.link.enabled.ports.only`	Se os switches retransmitem pacotes LLDP para o controlador apenas a partir de portas ativadas quando o controlador tenta descobrir links entre os switches. Valores possíveis: • `true` • `false`
`core.link.liveness.interval`	Intervalo, em milissegundos, para o controlador enviar pacotes LLDP através dos links do switch.
`core.link.liveness.timeout`	Intervalo, em milissegundos, para que o lado receptor dos links do switch receba pacotes LLDP e os encaminhe para o controlador. Se nenhum pacote LLDP chegar através do link dentro do tempo especificado, o controlador considera o link indisponível.
`core.lldp.sendrem.enabled`	Se os switches enviam notificações ao controlador sempre que as regras de fluxo que enviam pacotes de tráfego ao controlador são excluídas. Valores possíveis: • `true` • `false`
`core.switch.liveness.interval`	Intervalo, em milissegundos, para a verificação da conexão de switches ao controlador.
`core.switch.liveness.timeout`	Tempo, em milissegundos, dentro do qual os switches desconectados devem se reconectar ao controlador.
`core.tunnel.port.end`	Número da última interface de rede virtual (VNI) no intervalo de interfaces de switch.
`core.tunnel.port.start`	Número da primeira interface de rede virtual no intervalo de interfaces de switch.
`dampening.link.enabled`	Se Atenuação do link é usada. Valores possíveis: • `true` • `false`
`dampening.link.maxSuppressTime.ms`	Tempo máximo, em milissegundos, durante o qual o acesso ao link pode ser restringido. Quando o tempo especificado expirar, todos os contadores de Atenuação são redefinidos.
`dampening.link.penalty`	O número em que a Penalidade é incrementada quando o link muda de estado.

Propriedade	Descrição
`dampening.link.suppressLevel`	O valor da Penalidade em que o acesso ao link é restringido.
`dampening.link.updateInterval.ms`	Tempo, em milissegundos, dentro do qual a Penalidade deve atingir o valor `dampening.link.suppressLevel` para que o acesso ao link seja restringido.
`eth.s.type`	O valor TPID IEEE 802.1Q especificado como a tag interna para pacotes de tráfego com classificação de tráfego Q-in-Q.
`eth.t.type`	O valor TPID IEEE 802.1Q especificado como a tag externa para pacotes de tráfego com classificação de tráfego Q-in-Q.
`inband.statistics.enabled`	Obter estatísticas sobre switches. As estatísticas contêm informações sobre os dispositivos de rede aos quais o switch está conectado, bem como as portas sendo usadas. Valores possíveis: • `true` • `false`
`inband.swos.cookie`	Valor do campo `cookie` na mensagem para solicitação de estatísticas dos switches. Valores possíveis: • `true` • `false` Essa propriedade deve ser especificada se em `inband.statistics.enabled`, foi especificado `true`.
`network.control.queue.id`	ID da fila de pacotes LLDP nos switches.
`notification.all.queue.max.size`	Tamanho máximo da fila de notificações push nos switches. Se esse tamanho for excedido, a primeira notificação push na fila será excluída.
`openflow.fail2ban.banTimeSec`	Tempo, em segundos, durante o qual os endereços IP e as portas dos switches são bloqueados após uma tentativa de conexão ao controlador com um certificado TLS inválido.
`openflow.fail2ban.enabled`	Se os endereços IP e as portas dos switches são bloqueados após uma tentativa de conexão ao controlador com um certificado TLS inválido. Valores possíveis: • `true` • `false`
`openflow.fail2ban.findTimeSec`	Tempo, em segundos, dentro do qual os switches devem fazer o número de tentativas (especificado na propriedade `openflow.fail2ban.maxRetry`) de estabelecer conexão com o controlador com um certificado TLS inválido, o que faz com que os endereços IP e as portas desses switches sejam bloqueados.
`openflow.fail2ban.maxRetry`	O número de vezes que os switches tentam estabelecer conexão com o controlador com um certificado TLS inválido, após o que os endereços IP e as portas dos switches são bloqueados.
`openflow.io.cpe.rate.limiter.read.byteps`	Essa propriedade não é mais usada.
`openflow.io.cpe.rate.limiter.write.byteps`	Essa propriedade não é mais usada.
`openflow.io.ovs.meters.enabled`	Se as regras de fluxo enviam pacotes de tráfego para o controlador. Valores possíveis: • `true` • `false`
`openflow.io.rate.limiter.switch.type-to-rate`	Essa propriedade não é mais usada.
`openflow.io.switch.latency.monitoring.delay.ms`	Intervalo, em milissegundos, para verificar a latência entre o controlador e os switches.
`openflow.io.switch.latency.monitoring.enabled`	Se a latência é verificada entre o controlador e os switches. Valores possíveis: • `true` • `false`
`openflow.io.switch.latency.sma.initial.drop.size`	Número de pacotes de tráfego iniciais nos switches, que não é contabilizado nas estatísticas.
`openflow.io.switch.latency.sma.window.size`	Número de pacotes de tráfego finais nos switches, que não é contabilizado nas estatísticas.
`openflow.io.switch.messages.chunk.bytes`	Tamanho, em bytes, de blocos de mensagens OpenFlow serializadas que o controlador envia aos switches.

Propriedade	Descrição
`openflow.io.switch.messages.window.size`	Número máximo de blocos de mensagens OpenFlow serializadas na fila do controlador.
`openflow.io.switch.rate.limiter.read.byteps`	Essa propriedade não é mais usada.
`openflow.io.switch.rate.limiter.write.byteps`	Essa propriedade não é mais usada.
`openflow.io.vtep.rate.limiter.read.byteps`	Essa propriedade não é mais usada.
`openflow.io.vtep.rate.limiter.write.byteps`	Essa propriedade não é mais usada.
`segment.path.num.max`	Número máximo de caminhos em um segmento.
`segment.path.spf.num.max`	Número máximo de caminhos SPF para balanceamento automático.
`table-miss.mode`	Ação que os switches executam com pacotes de tráfego que não estão em nenhuma das tabelas OpenFlow. Valores possíveis: • `DROP` para descartar os pacotes de tráfego. • `TO_CTL` para enviar os pacotes de tráfego ao controlador.
`topology.cfm.enabled`	Se o Gerenciamento de falhas de conectividade (CFM) é usado em links. Valores possíveis: • `true` • `false`
`topology.debug.enabled`	Se as rotinas de depuração do controlador são usadas envolvendo o protocolo gRPC. Valores possíveis: • `true` • `false`
`topology.intervtep.links.enabled`	Estabelecer links entre VTEPs. Valores possíveis: • `true` • `false`
`topology.link.charged`	Usar todos os links como último recurso ao rotear o tráfego, independentemente da qualidade do link. Valores possíveis: • `true` • `false`
`topology.link.discovery.groups.enabled`	Descoberta de links por grupos. Valores possíveis: • `true` • `false`
`topology.link.encryption.enabled`	Criptografia de tráfego em links. Valores possíveis: • `true` • `false`
`topology.link.encryption.key.update.interval.minutes`	Intervalo em minutos para a atualização da chave de descriptografia nos links.
`topology.link.error.monitoring.enabled`	Monitoramento de erros nos links. Valores possíveis: • `true` • `false`
`topology.link.error.threshold.eps`	Limite de número de erros por segundo nos links.
`topology.link.eu.monitoring.delay.sec`	Intervalo, em segundos, para a medir o número de erros em links e a utilização do link.
`topology.link.fec.enable`	Se a Correção de erros de encaminhamento (FEC) é usada nos links. Valores possíveis: • `true` • `false`
`topology.link.fec.ratio`	Índice de pacotes de tráfego originais para pacotes adicionais com código redundante. Insira um valor no formato `<número de pacotes originais>:<número de pacotes adicionais>`.
`topology.link.fec.timeout`	Tempo máximo, em milissegundos, em que um pacote de tráfego pode permanecer na fila para a aplicação da FEC.
`topology.link.jitter.monitoring.enabled`	Monitoramento de jitter em links. Valores possíveis: • `true` • `false`

Propriedade	Descrição
`topology.link.jitter.threshold.ms`	Limite de tempo de jitter nos links, em milissegundos.
`topology.link.latency.monitoring.enabled`	Monitoramento da latência em links. Valores possíveis: • `true` • `false`
`topology.link.latency.threshold.ms`	Limite de latência em links, em milissegundos.
`topology.link.ljp.monitoring.delay.sec`	Intervalo, em segundos, para comparar os números de monitoramento recebidos com os limites especificados de latência, jitter e perda de pacotes nos links.
`topology.link.ljp.stats.collecting.enabled`	Monitoramento de latência, jitter e perda de pacotes de tráfego nos links. Valores possíveis: • `true` • `false` Para especificar o protocolo de monitoramento, use a propriedade `topology.link.ljp.stats.collecting.method`.
`topology.link.ljp.stats.collecting.lldp.window`	Tamanho em bytes do buffer adicional em cada pacote LLDP para os números de monitoramento de latência, jitter e perda de pacotes. Essa propriedade deve ser especificada se em `topology.link.ljp.stats.collecting.method`, foi especificado `GENEVE`.
`topology.link.ljp.stats.collecting.method`	Protocolo para monitoramento de latência, jitter e perda de pacotes de tráfego nos links. Valores possíveis: • `LLDP` • `GENEVE`
`topology.link.ljp.stats.collecting.multiplicity`	O multiplicador que o controlador aplica aos valores de monitoramento de atraso, jitter e perda de pacotes. Essa propriedade deve ser especificada se em `topology.link.ljp.stats.collecting.method`, foi especificado `GENEVE`.
`topology.link.packet.loss.monitoring.enabled`	Monitoramento da perda de pacotes de tráfego nos links. Valores possíveis: • `true` • `false`
`topology.link.packet.loss.threshold.percents`	Limite da porcentagem de perda de pacotes de tráfego nos links.
`topology.link.pmtud.scheduler.interval.sec`	Intervalo, em segundos, para a detecção automática do valor da MTU nos links.
`topology.link.pmtud.wait.time.ms`	Quanto tempo o controlador espera por um pacote LLDP de PMTUD, em milissegundos. Se o controlador não receber um pacote LLDP de PMTUD nesse período, ele conclui que um pacote desse tamanho não pode ser transmitido pelo link.
`topology.link.threshold.monitoring.delay.sec`	Intervalo, em segundos, para o monitoramento de limites de link.
`topology.link.threshold.monitoring.enabled`	Monitoramento de limite em links. Valores possíveis: • `true` • `false`
`topology.link.threshold.monitoring.unban.periods`	Número de verificações bem-sucedidas consecutivas para que um link seja desbloqueado. É executada uma verificação por segundo.
`topology.link.util.monitoring.enabled`	Monitoramento da utilização do link (uso da largura de banda). Valores possíveis: • `true` • `false`
`topology.link.util.threshold.percents`	Limite de utilização do link na forma de uma porcentagem da largura de banda das interfaces de serviço.
`topology.overlay.lldp.sender.concurrent`	Envio simultâneo de pacotes LLDP pelo controlador para descoberta de links. Valores possíveis: • `true` • `false`

Propriedade	Descrição
`topology.overlay.lldp.sender.core.pool.size`	Número mínimo de fluxos para o envio simultâneo de pacotes LLDP pelo controlador. Essa propriedade deve ser especificada se em `topology.overlay.lldp.sender.concurrent`, foi especificado `true`.
`topology.overlay.lldp.sender.max.pool.size`	Número máximo de fluxos para envio simultâneo de pacotes LLDP pelo controlador. Essa propriedade deve ser especificada se em `topology.overlay.lldp.sender.concurrent`, foi especificado `true`.
`topology.overlay.lldp.sender.max.queue.capacity`	Tamanho máximo da fila quando o controlador está enviando pacotes LLDP simultaneamente. Essa propriedade deve ser especificada se em `topology.overlay.lldp.sender.concurrent`, foi especificado `true`.
`topology.reserve.si.auto.revert.enabled`	A interface de serviço reserva volta a ser reserva se a interface de serviço antiga voltar a ficar operacional. Valores possíveis: • `true` • `false`
`topology.throttler.timeout.hard.enabled`	Acumulação de operações físicas no controlador, como conectar um switch ou uma porta, para executar as operações quando o tempo especificado tiver decorrido. Valores possíveis: • `true` • `false` Para especificar a hora, use as propriedades `topology.throttler.timeout.hard.ms` e `topology.throttler.timeout.idle.ms`.
`topology.throttler.timeout.hard.ms`	Tempo, em segundos, após o qual as operações físicas acumuladas no controlador são executadas. Essa propriedade deve ser especificada se em `topology.throttler.timeout.hard.enabled`, foi especificado `true`.
`topology.throttler.timeout.idle.ms`	Tempo, em segundos, após o qual as operações físicas acumuladas no controlador são executadas. A contagem reinicia sempre que uma operação física aparece. Essa propriedade pode ser especificada se em `topology.throttler.timeout.hard.enabled`, foi especificado `true`.
`topology.throttler_future.enable`	Propriedade do sistema. Editar esta propriedade pode tornar o controlador inoperável.
`topology.throttler_future.timeout.sec`	Propriedade do sistema. Editar esta propriedade pode tornar o controlador inoperável.

Editar uma propriedade do controlador

As alterações feitas nas propriedades do controlador com o método de alteração Tempo de execução começam a funcionar imediatamente. As alterações feitas nas propriedades do controlador com o método de alteração Recarregar começam a funcionar depois que o controlador é reiniciado.

Para alterar uma propriedade do controlador:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Propriedades** ao lado do controlador cuja propriedade deseja alterar.

   A página de propriedades do controlador é exibida. Por padrão, é selecionada a guia **Todas as propriedades**, que exibe uma tabela de todas as propriedades do controlador.

3. Selecione a guia **Propriedades alteráveis**.

   Uma tabela de propriedades editáveis do controlador é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado da propriedade do controlador que deseja editar.

5. Na janela aberta, no campo **Valor planejado**, insira o novo valor da propriedade.

6. Clique em **Salvar**.

O novo valor de uma propriedade com o método Tempo de execução é exibido na coluna **Valor atual**. O novo valor de uma propriedade com o método Recarregar é exibido na coluna **Valor planejado**.

Excluir valores planejados das propriedades do controlador

É possível excluir um valor planejado para desfazer uma alteração em uma propriedade do controlador. Esta ação se aplica apenas às propriedades que têm o método Recarregar.

Os valores planejados excluídos das propriedades do controlador não podem ser restaurados.

Para excluir valores planejados das propriedades do controlador:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. Clique em **Gerenciamento** → **Propriedades** ao lado do controlador para o qual deseja excluir os valores planejados das propriedades.

   A página de propriedades do controlador é exibida. Por padrão, é selecionada a guia **Todas as propriedades**, que exibe uma tabela de todas as propriedades do controlador.

3. Selecione a guia **Propriedades alteráveis**.

   Uma tabela de propriedades editáveis do controlador é exibida.

4. Exclua os valores planejados das propriedades do controlador de uma das seguintes formas:

   - Para excluir o valor planejado de uma única propriedade do controlador, clique em **Gerenciamento** → **Excluir valor planejado** ao lado da propriedade.

   - Para excluir os valores planejados de todas as propriedades do controlador, na parte superior da tabela, clique no ícone de configurações → **Excluir todos os valores planejados**.

5. Na janela de confirmação, clique em **Excluir**.

Os valores planejados das propriedades do controlador são excluídos.

Redefinir propriedades do controlador para os valores padrão

Para redefinir as propriedades do controlador para os valores padrão:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Propriedades** ao lado do controlador cujas propriedades deseja redefinir para os valores padrão.

   A página de propriedades do controlador é exibida. Por padrão, é selecionada a guia **Todas as propriedades**, que exibe uma tabela de todas as propriedades do controlador.

3. Selecione a guia **Propriedades alteráveis**.

   Uma tabela de propriedades editáveis do controlador é exibida.

4. Redefina as propriedades do controlador de uma das seguintes formas:

   - Para redefinir uma única propriedade do controlador para o valor padrão, clique em **Gerenciamento** → **Redefinir propriedade** ao lado da propriedade.

   - Para redefinir todas as propriedades do controlador para os valores padrão, clique no ícone de configurações na parte superior da tabela → **Redefinir todas as propriedades**.

5. Na janela de confirmação, clique em **Restaurar**.

As propriedades do controlador são redefinidas para os valores padrão.

Visualizar informações sobre nós do controlador

- Para visualizar informações sobre nós do controlador:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador cujas informações sobre nós deseja visualizar.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador. As informações sobre os nós do controlador são exibidas nas seguintes colunas da tabela:

   - **Endereço** é o endereço IP do nó do controlador.

   - **Status do nó** é o status dos nós do controlador:

     - **Conectado** significa que o nó está conectado ao controlador.

     - **Desconectado** significa que o nó não está conectado ao controlador.

- **Indisponível** significa que o nó não está disponível.
- **Desconhecido** significa que o status do nó é desconhecido.

- **Função no cluster** é a função do nó no cluster:
  - **Principal** significa que o nó está conectado ao controlador e é o nó principal do cluster.
  - **Secundário** significa que o nó está conectado ao controlador e é um nó secundário no cluster.
  - **Único** significa que o nó está conectado ao controlador e é o único nó no cluster.
  - **Árbitro** significa que o nó é o árbitro.
  - **Conectado (transição)** significa que a função do nó no cluster está sendo alterada.
  - **Não está em um cluster** significa que o nó não foi adicionado a um cluster.
  - **Indisponível** significa que o nó não está disponível.
  - **Desconhecido** significa que o status do nó é desconhecido.
- **Nó de leitura gRPC ativo** indica se o nó está selecionado como nó prioritário para operações de leitura para fins de balanceamento de carga.
- **Porta gRPC** é o número da porta gRPC do nó do controlador.
- **Porta JGroups** é o número da porta JGroups do nó do controlador.
- **Versão** é a versão do software do nó do controlador.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

3. Para visualizar as estatísticas de um nó do controlador, clique em**Gerenciamento** →**Estatísticas** ao lado do nó.
4. Para visualizar as propriedades de um nó do controlador, clique em **Gerenciamento** → **Propriedades do nó** ao lado do nó.

Gerenciar um VIM

É possível implementar um VIM em um dos data centers ou em um dispositivo uCPE. A implementação do VIM em um data center implica no gerenciamento centralizado do ciclo de vida da função de rede virtual. A implementação do VIM em um dispositivo uCPE permite entregar funções de rede virtual para data centers remotos e gerenciá-los localmente.

Para visualizar a tabela de VIMs, vá para a seção **Infraestrutura** do menu, clique no data center criado e selecione a guia **IPAM** → **Recursos de computação**. As informações sobre VIMs são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do VIM.
- **Tipo** é o tipo de VIM. O Kaspersky SD-WAN usa a plataforma de nuvem OpenStack como VIM.

- **Função** é o data center ou dispositivo uCPE em que o VIM está implementado.
- **IP do VIM** é o endereço IP do VIM.
- **Status** é o status da conexão do VIM com a plataforma de nuvem OpenStack:
  - **Conectado**.
  - **Desconectado**.
- **Cluster SDN** é o cluster SDN ao qual o OpenStack está conectado.
- **Atrás do NAT** permite especificar se o VIM está atrás da NAT (Conversão de endereço de rede):
  - **Sim**.
  - **Não**.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Configurar um VIM implementado em um data center

Para configurar um VIM implementado em um data center:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. No painel **Recursos**, selecione o domínio criado e, em seguida, o data center adicionado no qual o VIM foi implementado.

3. Selecione a guia **Recursos de computação**.

   Uma tabela de VIMs é exibida.

4. Na parte superior da página, clique em **+ VIM**.

5. Na janela aberta, no campo **Nome**, insira o nome do VIM.

6. No campo **Endereço IP**, insira o endereço IP ou nome de domínio para conectar o orquestrador ao VIM.

7. No campo **Porta**, insira o número da porta para conectar o orquestrador ao serviço de identificação VIM. O valor padrão é `5000`.

8. Na lista suspensa **Protocolo**, selecione o protocolo para conectar o orquestrador ao VIM:
   - **http**. Esse é o nível padrão.
   - **https**.

9. Nos campos **Login** e **Senha**, insira o nome de usuário e a senha de uma conta com privilégios de administrador para autenticar o orquestrador na plataforma de nuvem OpenStack. Se a autenticação for bem-sucedida, o orquestrador obtém acesso ao gerenciamento da infraestrutura virtual que está disponível para o administrador.

10. Especifique as configurações avançadas de autenticação do orquestrador na plataforma de nuvem OpenStack:

    a. No campo **Projeto do administrador**, insira o nome do projeto do administrador para autenticação do orquestrador no projeto do administrador.

    b. No campo **Domínio**, insira o nome de domínio do OpenStack para a autenticação do orquestrador nele.

11. Na lista suspensa **Atrás do NAT**, selecione se o VIM está atrás do NAT:

    - **Ativado** para indicar que o VIM está atrás do NAT e a conversão do endereço de rede ocorre quando o VIM interage com a instância SD-WAN.
    - **Desativado** para indicar que o VIM não está atrás do NAT. Esse é o padrão.

12. Especifique as taxas de superalocação para recursos físicos:

    a. No campo **Superalocação de CPU**, insira a taxa de superalocação do núcleo da CPU. O valor padrão é `1`.

    b. No campo **Superalocação de RAM**, insira a taxa de superalocação da RAM. O valor padrão é `1`.

    c. No campo **Superalocação de disco**, insira a taxa de superalocação do espaço em disco. O valor padrão é `1`.

    As taxas de superalocação permitem provisionar máquinas virtuais com mais recursos virtuais do que os fisicamente presentes. Isso é possível porque as máquinas virtuais não usam simultaneamente todos os recursos físicos disponíveis ao máximo. Por exemplo, ao especificar um fator de superalocação do espaço em disco de `3`, o espaço em disco virtual disponível pode ser três vezes maior que o espaço em disco fisicamente disponível no host.

    Ao configurar a superalocação, considere como os recursos do hardware se relacionam com os requisitos das máquinas virtuais. Caso seja especificada uma taxa de superalocação alta para recursos físicos e as máquinas virtuais os usarem, isso pode levar ao atraso da rede e/ou fazer com que partes da rede se tornem completamente indisponíveis.

13. No campo **Paralelismo**, insira o número máximo de operações simultâneas entre o orquestrador e o VIM. O valor padrão é `1`. Essa configuração permite reduzir o tempo de processamento geral das operações, mas cria uma carga adicional na infraestrutura virtual.

    Recomendamos não alterar o valor padrão, a menos que a velocidade geral de processamento da operação seja crítica.

14. Na lista suspensa **Cluster SDN**, selecione o cluster SDN ao qual o OpenStack está conectado. Se o OpenStack não estiver conectado a nenhum cluster SDN, selecione**Nenhum**.

15. No campo **Número máximo de VLANs**, insira o número máximo de VLANs que o VIM pode usar. Essa configuração permite que o orquestrador acompanhe o número de segmentos disponíveis para uso. Intervalo de valores: 0 a 4.094.

16. Se o VIM for compatível com SR-IOV, insira o nome physnet no campo **Rede física SR-IOV**. O orquestrador usa o nome da rede física SR-IOV para estabelecer a conexão de máquinas virtuais com o tipo de interface SR-IOV.

17. Caso esteja usando uma rede com o tipo de segmentação VLAN para gerenciamento, no campo **Rede física VLAN**, insira a tag VLAN.

18. Caso tenha selecionado um cluster SDN na lista suspensa **Cluster SDN**, configure a conexão com esse cluster:

    a. Para mapear as redes lógicas da instância SD-WAN para uma rede física, insira o nome physnet no campo **Rede física do OpenStack**.

    b. Na lista suspensa **Grupo de portas**, selecione o grupo de portas através do qual todos os nós do OpenStack estão conectados ao cluster SDN.

    c. Na lista suspensa **Grupo de controle**, selecione o grupo de portas através do qual os nós de controle do OpenStack estão conectados ao cluster SDN.

    d. Se necessário, na lista suspensa **Grupo de computação**, selecione o grupo de portas através do qual os nós de computação do OpenStack estão conectados ao cluster SDN.

19. Caso tenha selecionado **Nenhum** na lista suspensa **Cluster SDN**, configure a rede:

    a. Para mapear as redes simples da instância SD-WAN para uma rede física, insira o nome physnet no campo **Rede física plana**.

    b. Para mapear a VXLAN da instância SD-WAN para uma rede física, insira o nome physnet no campo **Rede física VXLAN**.

    c. Na lista suspensa **Segmentação da rede de controle**, selecione o tipo de segmentação para isolar e proteger o tráfego do plano de controle na estrutura SD-WAN:

    - **VLAN**
    - **VXLAN**

    d. No campo **ID do segmento de controle**, insira o ID de segmento da rede de gerenciamento. O intervalo de valores depende do valor selecionado na lista suspensa **Segmentação da rede de controle**:

    - Se **VLAN** for selecionado, o intervalo de valores é de 0 a 4.095.
    - Se **VXLAN** for selecionado, o intervalo de valores é de 0 a 16.000.000.

    e. Na lista suspensa **Segurança de portas**, selecione se deseja ativar a função Segurança da porta:

    - **Ativado**
    - **Desativado**

    f. No campo **Permitir CIDR**, insira o prefixo IPv4 da sub-rede permitida para a rede de gerenciamento.

20. Clique em **Criar**.

O VIM é criado e exibido na tabela na guia **Recursos de computação**.

Configurar um VIM implementado em um dispositivo uCPE

Para configurar um VIM implementado em um dispositivo uCPE, especifique as configurações do VIM em um modelo de uCPE. As configurações de VIM especificadas em um modelo de uCPE são aplicadas automaticamente a todos os dispositivos CPE que usam o modelo.

Para configurar um VIM implementado em um dispositivo uCPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de uCPE no qual deseja configurar um VIM.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Selecione a guia **VIM**.

   As configurações do VIM são exibidas.

4. No campo **Porta**, insira o número da porta para conectar o orquestrador ao serviço de identificação VIM. O valor padrão é `5000`.

5. Na lista suspensa **Protocolo**, selecione o protocolo para conectar o orquestrador ao VIM:

   - **http**. Esse é o nível padrão.
   - **https**.

6. Nos campos **Login** e **Senha**, insira o nome de usuário e a senha de uma conta com privilégios de administrador para autenticar o orquestrador na plataforma de nuvem OpenStack. Se a autenticação for bem-sucedida, o orquestrador obtém acesso ao gerenciamento da infraestrutura virtual que está disponível para o administrador.

7. Especifique as configurações avançadas de autenticação do orquestrador na plataforma de nuvem OpenStack:

   a. No campo **Projeto do administrador**, insira o nome do projeto do administrador para autenticação do orquestrador no projeto do administrador.

   b. No campo **Domínio**, insira o nome de domínio do OpenStack para a autenticação do orquestrador nele.

8. Caso esteja usando uma rede com o tipo de segmentação VLAN para gerenciamento, no campo **Rede física VLAN**, insira a tag VLAN.

9. Na lista suspensa **Atrás do NAT**, selecione se o VIM está atrás do NAT:

   - **Ativado** para indicar que o VIM está atrás do NAT e a conversão do endereço de rede ocorre quando ele interage com a instância SD-WAN.
   - **Desativado** para indicar que o VIM não está atrás do NAT. Esse é o padrão.

10. Especifique as taxas de superalocação para recursos físicos:

    a. No campo **Superalocação de CPU**, insira a taxa de superalocação do núcleo da CPU. O valor padrão é `1`.

    b. No campo **Superalocação de RAM**, insira a taxa de superalocação da RAM. O valor padrão é `1`.

    c. No campo **Superalocação de disco**, insira a taxa de superalocação do espaço em disco. O valor padrão é `1`.

    As taxas de superalocação permitem provisionar máquinas virtuais com mais recursos virtuais do que os fisicamente presentes. Isso é possível porque as máquinas virtuais não usam simultaneamente todos os recursos físicos disponíveis ao máximo. Por exemplo, ao especificar um fator de superalocação do espaço em disco de `3`, o espaço em disco virtual disponível pode ser três vezes maior que o espaço em disco fisicamente disponível no host.

    Ao configurar a superalocação, considere como os recursos do hardware se relacionam com os requisitos das máquinas virtuais. Caso seja especificada uma taxa de superalocação alta para recursos físicos e as máquinas virtuais os usarem, isso pode levar ao atraso da rede e/ou fazer com que partes da rede se tornem completamente indisponíveis.

11. No campo **Número máximo de VLANs**, insira o número máximo de VLANs que o VIM pode usar. Essa configuração permite que o orquestrador acompanhe o número de segmentos disponíveis para uso. Intervalo de valores: 0 a 4.094.

12. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE.

Editar um VIM implementado em um data center

Para editar um VIM implementado em um data center:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. No painel **Recursos**, selecione o domínio criado e, em seguida, o data center adicionado no qual o VIM foi implementado.

3. Selecione a guia **Recursos de computação**.

   Uma tabela de VIMs é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do VIM que deseja editar.

5. Na janela aberta, se necessário, edite as configurações do VIM. Para obter uma descrição das configurações, consulte as instruções para configurar um VIM implementado em um data center.

6. Clique em **Salvar**.

O VIM é modificado e atualizado na tabela.

Visualizar recursos de computação sendo usados por um VIM

É possível visualizar a utilização dos seguintes recursos de computação pelo VIM:

- CPU
- RAM
- Espaço em disco
- Segmentos de rede

Para visualizar os recursos de computação usados pelo VIM:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. No painel **Recursos**, selecione o domínio criado e, em seguida, o data center adicionado no qual o VIM foi implementado.

3. Selecione a guia **Recursos de computação**.

   Uma tabela de VIMs é exibida.

4. Clique em **Gerenciamento** → **Mostrar utilização** ao lado do VIM.

Isso abre uma janela com informações sobre os recursos de computação usados pelo VIM.

Excluir um VIM

VIMs excluídos não podem ser restaurados.

Para excluir um VIM:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. No painel **Recursos**, selecione o domínio criado e, em seguida, o data center adicionado no qual o VIM foi implementado.

3. Selecione a guia **Recursos de computação**.

   Uma tabela de VIMs é exibida.

4. Clique em **Gerenciamento** → **Excluir** ao lado do VIM que deseja excluir.

5. Na janela de confirmação, clique em **Excluir**.

O VIM é excluído e não é mais exibido na tabela.

Gerenciar usuários e suas permissões de acesso

Para restringir o acesso ao portal do administrador e ao portal de autoatendimento, bem como a seções, subseções e funções, a solução implementa um modelo de Controle de acesso baseado em função (RBAC). As contas de usuário podem ter as seguintes funções:

- Um administrador tem acesso ao portal do administrador e ao portal de autoatendimento.
- Um locatário tem acesso apenas ao portal de autoatendimento.

Implementar a solução cria o usuário **Administrador** com a função de administrador e o usuário **Usuário** com a função de locatário.

É possível criar usuários locais, usuários LDAP e grupos de usuários LDAP. A solução não é compatível com a criação de grupos de usuários locais. As credenciais de usuários locais são armazenadas no banco de dados do orquestrador. As credenciais de usuários LDAP e grupos de usuários LDAP são armazenadas em um servidor remoto. Os servidores compatíveis incluem o servidor OpenLDAP remoto com autenticação SSL simples, bem como o Microsoft Active Directory com autenticação Kerberos e Kerberos SSL.

É necessário primeiro criar uma conexão LDAP que o orquestrador usa para se conectar ao servidor remoto e, em seguida, criar usuários LDAP e/ou grupos de usuários LDAP. Os usuários e grupos de usuários LDAP criados podem fazer login na interface da Web do orquestrador usando suas credenciais.

Autenticação de dois fatores

Para melhorar o nível de segurança geral da solução, é possível solicitar a autenticação de dois fatores dos usuários usando o algoritmo de senha de uso único baseada em tempo (TOTP). É possível ativar ou desativar a autenticação de dois fatores para todos os usuários. Também é possível ativar ou desativar a autenticação de dois fatores ao criar ou editar usuários locais, usuários LDAP e grupos LDAP.

Se a autenticação de dois fatores estiver ativada para um usuário, um código QR exclusivo será gerado na próxima vez que o usuário fizer login na interface da Web do orquestrador. O usuário deve digitalizar o código QR usando um autenticador de software ou hardware compatível com RFC 6238, como o Kaspersky Password Manager, Google Authenticator, Yandex Key e Microsoft Authenticator. O autenticador gera um código único que o usuário deve inserir para concluir a autenticação de dois fatores e fazer login na interface da Web do orquestrador. Se o código único for inserido incorretamente mais de cinco vezes, o usuário é bloqueado por 30 minutos.

Após concluir a autenticação de dois fatores, o usuário deve inserir um nome de usuário, senha e um código exclusivo para fazer login na interface da Web do orquestrador. Se necessário, é possível pedir que o usuário conclua a autenticação de dois fatores novamente.

> Se a discrepância de tempo entre o orquestrador e o autenticador for superior a 30 segundos, a autenticação de dois fatores pode falhar. Recomendamos sincronizar a hora no orquestrador e no autenticador usando um servidor NTP.

Permissões de acesso

Se necessário, é possível criar permissões de acesso que determinem que seções e subseções da interface da Web do orquestrador e que ações estão disponíveis para quais usuários, além de atribuir permissões de acesso ao criar ou editar usuários e grupos LDAP. Por exemplo, uma permissão de acesso que proíbe o acesso à seção **Catálogo** e a criação de modelos de serviço de rede.

Por padrão, os usuários e grupos LDAP têm a permissão **Acesso total**, que concede acesso total a todas as funcionalidades da solução.

Solicitações de confirmação

Ao criar ou editar um usuário, especifique se deseja que uma solicitação de confirmação seja criada automaticamente sempre que esse usuário executar uma ação. As solicitações de confirmação podem ser confirmadas, negadas ou excluídas. Quando uma solicitação é confirmada, a ação associada é executada. Solicitações de confirmação negadas são salvas na interface da Web do orquestrador.

Sessões de usuário

A seguinte funcionalidade é usada para gerenciar sessões do usuários:

- Limitar a duração das sessões de usuário. Se um usuário permanece ocioso por 3600 segundos (uma hora) após fazer login na interface da Web do orquestrador, a sessão do usuário é encerrada automaticamente. É possível especificar manualmente o tempo ocioso antes do logout automático.
- Encerramento de sessões do usuários. Se vários funcionários usarem as mesmas credenciais de conta de usuário para fazer login na interface da Web do orquestrador, qualquer um desses funcionários poderá encerrar as sessões dos outros.

Gerenciar permissões de acesso

É possível exibir a lista de permissões de acesso na seção **Usuários**, na guia **Permissões**. Por padrão, é criada a permissão de **Acesso total**, que concede acesso total à interface da Web do orquestrador e é automaticamente atribuída a usuários e grupos de usuários LDAP caso não seja atribuída uma permissão de acesso diferente a eles.

As ações que podem ser executadas com a lista são descritas nas instruções Gerenciar tabelas de componentes da solução.

Criar permissões de acesso

Para criar uma permissão de acesso:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Permissões**.

   A lista de permissões de acesso é exibida.

3. Na parte superior da lista, clique em **+ Permissão**.

4. Na área de configurações exibida, no campo **Nome**, insira o nome da permissão de acesso. O comprimento máximo do nome é de 250 caracteres.

5. Na seção **Direitos de acesso** ao lado das seções e subseções da interface da Web do orquestrador, selecione um dos seguintes valores:

   - **Editar** para permitir que os usuários visualizem a seção ou subseção e executem todas as tarefas disponíveis nela.
   - **Visualizar** para permitir que os usuários apenas visualizem a seção ou subseção.
   - **Sem acesso** para impedir que os usuários visualizem a seção ou subseção.

   Caso deseje que as subseções herdem o valor selecionado para a seção, marque a caixa de seleção **Aplicar a subseções**. Esta caixa de seleção está desmarcada por padrão.

6. Clique em **Criar**.

A permissão de acesso é criada e exibida na lista.

É possível atribuir uma permissão de acesso ao criar ou editar um usuário, ou ao criar ou editar um grupo de usuários LDAP.

Editar permissões de acesso

Para editar uma permissão de acesso:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Permissões**.

   A lista de permissões de acesso é exibida.

3. Clique na permissão de acesso que deseja editar.

4. Na área de configurações exibida, edite as seguintes configurações, se necessário:

   - Nome da permissão de acesso
   - Seções e subseções da interface da Web do orquestrador e ações disponíveis para os usuários

5. Clique em **Salvar**.

A permissão de acesso é modificada e atualizada na lista.

Clonar permissões de acesso

É possível clonar uma permissão de acesso para criar uma permissão idêntica com um nome diferente.

Para clonar uma permissão de acesso:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Permissões**.

   A lista de permissões de acesso é exibida.

3. Clique na permissão de acesso que deseja clonar.

4. Na parte superior da área de configurações exibida, clique em **Gerenciamento** → **Clonar**.

5. Na janela aberta, insira o nome da nova permissão de acesso.

6. Clique em **Clonar**.

Um clone da permissão de acesso com o novo nome é criado e adicionado à lista.

Remover uma permissão de acesso

As permissões de acesso excluídas não podem ser restauradas.

Para remover uma permissão de acesso:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Permissões**.

   A lista de permissões de acesso é exibida.

3. Clique na permissão de acesso que deseja excluir.

4. Na parte superior da área de configurações exibida, clique em **Gerenciamento**→ **Excluir**.

5. Na janela de confirmação, clique em **Excluir**.

A permissão de acesso é excluída e não é mais exibida na lista.

Gerenciar conexões LDAP

Consulte a tabela de conexões LDAP na seção **Usuários**, na guia **Conexões LDAP**. As informações sobre conexões LDAP são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da conexão LDAP.
- **Tipo** é o tipo de conexão. Essa coluna sempre exibe **LDAP**.
- **Host** é o nome do host do servidor remoto.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar uma conexão LDAP

Caso deseje que usuários LDAP ou grupos de usuários LDAP possam fazer login na interface da Web do orquestrador usando suas credenciais, primeiro crie uma conexão LDAP que o orquestrador usará para se conectar ao servidor remoto e, em seguida, crie os usuários LDAP ou grupos de usuários LDAP.

Para criar uma conexão LDAP:

1. No menu, vá para a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Conexões LDAP**.

   Uma tabela de conexões LDAP é exibida.

3. Clique em **+ LDAP**.

4. Na área de configurações exibida, no campo **Nome**, insira o nome da conexão LDAP.

5. No campo **Domínio**, insira o FQDN do domínio do servidor remoto.

6. No campo **Alias do domínio**, insira o alias ou o nome NETBIOS do domínio. Os usuários inserem o alias, o nome NETBIOS ou o FQDN do domínio ao fazer login na interface da Web do orquestrador.

   Por exemplo, se o FQDN do domínio for 'exemplo.com' e o alias for 'exemplo', um usuário denominado 'admin' pode inserir as seguintes credenciais ao fazer login na interface da Web do orquestrador:

   - `admin@exemplo.com`
   - `admin@exemplo`
   - `exemplo.com\admin`
   - `exemplo\admin`

7. No campo **Host LDAP**, insira o nome do host do servidor remoto. Os seguintes formatos de nome do host são compatíveis:

   - `ldap://<nome do host>:<número da porta>` para um servidor LDAP padrão. A porta padrão é 389.
   - `ldaps://<nome do host>:<número da porta>` para um servidor LDAP com autenticação SSL. A porta padrão é 636.

   Por exemplo, ao inserir `ldap://exemplo.com:100`, o nome do host do servidor remoto é 'exemplo.com' e o número da porta é 100.

8. No campo **DN da base**, insira o nome diferenciado base que o orquestrador usa como ponto de partida para pesquisar contas de usuário no diretório do servidor remoto. Os seguintes formatos de nome diferenciado base são compatíveis:

   - Para pesquisar no OpenLDAP, insira o nome diferenciado base no formato `OU=<valor>,OU=<valor>`, em que `OU` é a estrutura de unidades organizacionais no diretório do servidor remoto. Por exemplo, ao inserir `OU=OU_exemplo1,OU=OU_exemplo2`, o ponto de partida para pesquisar contas de usuário será a unidade organizacional OU_exemplo2, que está aninhada em OU_exemplo1.
   - Para pesquisar no Microsoft Active Directory, insira o nome diferenciado base no formato `DC=<valor>,DC=<valor>`, em que os `DCs` são os componentes de domínio do servidor remoto. Por exemplo, ao inserir `DC=exemplo,DC=com`, o ponto de partida para pesquisar contas de usuário será o domínio 'exemplo.com'.

9. Na lista suspensa **Pesquisar atributo**, selecione o atributo que o orquestrador usa para pesquisar contas de usuário no diretório do servidor remoto:

   - **uid (OpenLDAP)** é o UID (ID do usuário) para pesquisar no OpenLDAP. Essa é a configuração padrão.
   - **sAMAccountName (Active Directory)** é o nome de logon anterior ao Windows 2000 para pesquisar no Microsoft Active Directory.

10. No campo **DN de vinculação**, insira o nome diferenciado para autenticar o orquestrador no servidor remoto. Os seguintes formatos de nome diferenciado são compatíveis:

    - Para autenticação no openLDAP, insira um valor no formato `UID=<valor>`, `OU=<valor>`, em que `UID` é o ID do usuário e `OU` é a estrutura da unidade organizacional no diretório do servidor remoto onde o usuário está localizado. Por exemplo, ao inserir `UID=usuário_exemplo,OU=OU_exemplo`, o usuário usuário_exemplo da unidade organizacional OU_exemplo é usado para autenticar o orquestrador no servidor remoto.
    - Para autenticação no Microsoft Active Directory, insira um valor no formato `CN=<valor>`, `OU=<valor>`, `DC=<valor>`, `DC=<valor>`, em que `CN` é o nome comum do usuário, `OU` é a estrutura da unidade organizacional no diretório do servidor remoto ao qual o usuário pertence e os `DCs` são os componentes de domínio do usuário. Por exemplo, ao inserir `CN=usuário_exemplo,OU=OU_exemplo,DC=exemplo,DC=com`, o usuário usuário_exemplo na unidade organizacional OU_exemplo no domínio exemplo.com é usado para autenticar o orquestrador no servidor remoto.

11. No campo **Senha de vinculação**, insira a senha do servidor remoto para autenticar o orquestrador no servidor remoto. Para ver a senha inserida, clique no ícone de exibição 👁.

12. Para verificar se o servidor remoto está disponível, clique em **Testar autenticação**.

13. Clique em **Criar**.

A conexão LDAP é criada e exibida na tabela.

Editar uma conexão LDAP

Para editar uma conexão LDAP:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Conexões LDAP**.

   Uma tabela de conexões LDAP é exibida.

3. Clique na conexão LDAP que deseja editar.

4. Na área exibida, edite as seguintes configurações de conexão LDAP, se necessário: para obter uma descrição das configurações, consulte as instruções para criar uma conexão LDAP.

5. Clique em **Salvar**.

A conexão LDAP é modificada e atualizada na tabela.

Alterar a senha de uma conexão LDAP

É possível alterar a senha do servidor remoto especificada quando a conexão LDAP foi criada e fazer com que o orquestrador use a nova senha para fazer a autenticação com o servidor remoto.

Para alterar a senha de uma conexão LDAP:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Conexões LDAP**.

   Uma tabela de conexões LDAP é exibida.

3. Clique na conexão LDAP para a qual deseja alterar a senha.

4. Na parte superior da área de configurações exibida, clique no botão **Gerenciamento** → **Alterar a senha**.

5. Na janela aberta, digite a nova senha nas caixas de texto **Nova senha** e **Confirmar a senha**.

6. Clique em **Salvar**.

A senha da conexão LDAP é alterada.

Excluir uma conexão LDAP

As conexões LDAP excluídas não podem ser restauradas.

Para excluir uma conexão LDAP:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Conexões LDAP**.

   Uma tabela de conexões LDAP é exibida.

3. Clique na conexão LDAP que deseja excluir.

4. Na parte superior da área de configurações exibida, clique em **Gerenciamento**→ **Excluir**.

5. Na janela de confirmação, clique em **Excluir**.

A conexão LDAP é excluída e não é mais exibida na tabela.

Gerenciar usuários

É possível visualizar a tabela de usuário na seção **Usuários**. As informações sobre os usuários são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do usuário.
- **Locatário** é o locatário ao qual o usuário está atribuído.
- **Função** é a função do usuário:
  - **Administrador**
  - **Locatário**
- **Origem** é o tipo de usuário:
  - **Local** é um usuário local.
  - **LDAP** é um usuário LDAP.
- **Grupo** é o grupo do usuário LDAP. Se o usuário for local, a coluna exibe **Padrão**.

- **Estado** é o status do usuário:
  - **On-line**
  - **Offline**
  - **Bloqueado**
- **Autenticação de dois fatores** especifica se a autenticação de dois fatores está ativada para o usuário:
  - **Ativado** significa que a autenticação de dois fatores está ativada para o usuário.
  - **Desativado** significa que a autenticação de dois fatores está desativada para o usuário.
  - **Reinicialização** significa que é executada uma autenticação de dois fatores repetida para o usuário.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um usuário

É possível criar usuários locais e LDAP. As credenciais de usuários locais são armazenadas no banco de dados do orquestrador. As credenciais do usuário LDAP são armazenadas no servidor remoto. Caso deseje que usuários LDAP possam fazer login na interface da Web do orquestrador usando suas credenciais, primeiro crie uma conexão LDAP que o orquestrador usará para se conectar ao servidor remoto e, em seguida, crie os usuários LDAP ou grupos de usuários LDAP.

Para criar um usuário:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Clique em **+ Usuário**.

3. Na área de configurações exibida, na lista suspensa **Tipo de conta**, selecione o tipo de usuário:

   - **Local**. Essa é a configuração padrão. Se esse valor for selecionado nos campos **Senha** e **Confirmar a senha**, insira a senha do usuário. A senha deve conter pelo menos uma letra latina maiúscula (A–Z), uma letra minúscula (a–z), um número e um caractere especial. Comprimento da senha: 8 a 50 caracteres. Para ver a senha inserida, clique no ícone de exibição 👁.
   - **LDAP**.
   - **Serviço**

4. No campo **Nome de usuário**, insira o nome de usuário do usuário. O nome de usuário do servidor remoto é especificado no formato `usuário@domínio` ou `domínio\usuário`.

5. Na lista suspensa **Função**, selecione a função do usuário:

   - **Administrador**
   - **Locatário**

- **Restricted-API-extern-ISU**

  Essa função é usada para integrar o Kaspersky SD-WAN com ferramentas externas de segurança da informação por meio da API do orquestrador.

6. Na lista suspensa **Permissões**, selecione a permissão de acesso criada que deseja atribuir ao usuário. Por padrão, o usuário recebe a permissão de **Acesso total**, que concede acesso total à interface da Web do orquestrador.

7. Para ativar a autenticação de dois fatores para o usuário, marque a caixa de seleção **Autenticação de dois fatores**. Esta caixa de seleção está desmarcada por padrão. O usuário deve concluir a autenticação de dois fatores na próxima vez que fizer login na interface da Web do orquestrador.

   Não é possível ativar a autenticação de dois fatores para um usuário individual se ela estiver desativada para todos os usuários.

8. Para criar uma solicitação de confirmação sempre que o usuário executar uma ação, marque a caixa de seleção **Confirmação de solicitação obrigatória**. Essa caixa de seleção fica desmarcada por padrão e o usuário pode executar ações sem confirmação.

9. No campo **Nome**, insira o primeiro nome do funcionário.

10. No campo **Sobrenome**, insira o sobrenome do funcionário.

11. Se necessário, insira informações adicionais sobre o usuário:

    a. No campo **E-mail**, insira o endereço de e-mail.

    b. No campo **Descrição**, insira uma breve descrição do usuário.

12. Clique em **Criar**.

O usuário é criado e exibido na tabela. Por padrão, o usuário é bloqueado.

Desbloqueie o usuário para conceder a ele acesso à interface da Web do orquestrador.

Ativar ou bloquear um usuário

Por padrão, os usuários criados são bloqueados. Desbloqueie o usuário para conceder a ele acesso à interface da Web do orquestrador.

Para bloquear ou desbloquear um usuário:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Clique no usuário que deseja desbloquear ou bloquear.

3. Na parte superior da área de configurações exibida, clique em **Gerenciamento** → **Desbloquear** ou **Bloquear**.

O usuário é desbloqueado ou bloqueado.

Editar um usuário

Não é possível alterar o tipo e o nome do usuário. Há instruções separadas para alterar a senha de um usuário local.

Para editar um usuário:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione o usuário que deseja editar.

3. Na área exibida, edite as configurações de usuário, se necessário. Para obter uma descrição das configurações, consulte as instruções para criar um usuário.

4. Clique em **Salvar**.

O usuário é modificado e atualizado na tabela.

Alterar a senha de um usuário local

As senhas de usuários LDAP são armazenadas em servidores remotos e não podem ser alteradas na interface da Web do orquestrador.

Para alterar a senha de um usuário local:

1. Altere a senha do usuário local:

   - Se você tiver a função de administrador da plataforma e quiser alterar a senha do usuário local criado, vá para a seção **Usuários** do menu, clique no usuário local e clique em **Gerenciamento** → **Alterar a senha**.

   - Se você tiver a função de locatário e quiser alterar sua própria senha, na parte inferior do menu, clique no ícone de configurações → **Alterar a senha**.

2. Na janela aberta, digite a nova senha nas caixas de texto **Nova senha** e **Confirmar a senha**. A senha deve conter pelo menos uma letra latina maiúscula (A–Z), uma letra minúscula (a–z), um número e um caractere especial. Comprimento da senha: 8 a 50 caracteres. Para ver a senha inserida, clique no ícone de exibição .

3. Clique em **Salvar**.

A senha do usuário local é alterada.

Autenticação de dois fatores repetida de um usuário

É possível fazer com que o usuário repita a autenticação caso ele tenha perdido o acesso ao código exclusivo para fazer login na interface da Web do orquestrador gerada como resultado da autenticação de dois fatores anterior.

Para repetir a autenticação do usuário:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Clique no usuário que deseja autenticar novamente com a autenticação de dois fatores.

3. Na parte superior da área de configurações exibida, clique em **Gerenciamento** → **Reinicializar 2FA**.

O usuário deve concluir a autenticação de dois fatores na próxima vez que fizer login na interface da Web do orquestrador.

Excluir uma conta de usuário

Os usuários excluídos não podem ser restaurados.

Para excluir um usuário:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione o usuário que deseja excluir.

3. Na parte superior da área de configurações exibida, clique em **Gerenciamento** → **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

O usuário é excluído e não é mais exibido na tabela.

Gerenciar grupos de usuários LDAP

É possível visualizar a tabela de grupos de usuários LDAP na seção **Usuários**, na guia **Grupos**. As informações sobre os grupos de usuários LDAP são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do grupo de usuários LDAP.
- **Locatário** é o locatário ao qual o grupo de usuários LDAP está atribuído.
- **Função** é a função dos usuários LDAP.
- **Tipo** é o tipo de grupo de usuários. O Kaspersky SD-WAN só é compatível com grupos de usuários LDAP.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um grupo de usuários LDAP

As credenciais do grupo de usuários LDAP são armazenadas no servidor remoto. Caso deseje que os usuários no grupo de usuários LDAP possam fazer login na interface da Web do orquestrador usando suas credenciais, primeiro crie uma conexão LDAP que o orquestrador usará para se conectar ao servidor remoto e, em seguida, crie os usuários LDAP ou grupos de usuários LDAP.

> Se o usuário for membro de vários grupos de usuários LDAP no servidor remoto, recomendamos criar apenas um desses grupos na interface da Web do orquestrador. Se vários grupos de usuários LDAP tiverem sido criados na interface da Web do orquestrador, um usuário que for membro de todos esses grupos fará login na interface da Web do orquestrador como membro do grupo de usuários LDAP que foi criado primeiro.

Para criar um grupo de usuários LDAP:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Grupos**.

   Uma tabela de grupos de usuários LDAP é exibida.

3. Clique em **+ Adicionar**.

4. Na área de configurações exibida, no campo **Nome**, insira o nome do grupo de usuários LDAP no servidor remoto no formato `usuário@domínio` ou `domínio\usuário`.

5. Na lista suspensa **Função**, selecione a função dos usuários LDAP no grupo:

   - **Administrador**
   - **Locatário**

6. Na lista suspensa **Permissões**, selecione a permissão de acesso criada que deseja atribuir ao grupo de usuários LDAP. Por padrão, o grupo de usuários LDAP recebe a permissão de **Acesso total**, que concede acesso total à interface da Web do orquestrador.

7. Para ativar a autenticação de dois fatores para o grupo de usuários LDAP, marque a caixa de seleção **Autenticação de dois fatores**. Esta caixa de seleção está desmarcada por padrão. Os usuários no grupo de usuários LDAP devem concluir a autenticação de dois fatores na próxima vez que fizerem login na interface da Web do orquestrador.

   Quando a autenticação de dois fatores é ativada para um grupo de usuários LDAP, os usuários LDAP autenticados são exibidos na tabela de usuários. É possível desativar a autenticação de dois fatores para um usuário LDAP editando o usuário.

   Não é possível ativar a autenticação de dois fatores para um grupo de usuários LDAP se ela estiver desativada para todos os usuários.

8. Clique em **Criar**.

O grupo de usuários LDAP é criado e exibido na tabela.

Editar um grupo de usuários LDAP

Não é possível alterar o tipo e o nome do grupo de usuários LDAP.

Para editar um grupo de usuários:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Grupos**.

   Uma tabela de grupos de usuários LDAP é exibida.

3. Clique no grupo de usuários LDAP que deseja editar.

4. Na área de configurações exibida, edite as seguintes configurações do grupo de usuários LDAP, se necessário: para obter uma descrição das configurações, consulte as instruções para criar um grupo de usuários LDAP.

5. Clique em **Salvar**.

O grupo de usuários LDAP é modificado e atualizado na tabela.

Excluir um grupo de usuários LDAP

Os grupos de usuários LDAP excluídos não podem ser restaurados.

Para excluir um grupo de usuários LDAP:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Grupos**.

   Uma tabela de grupos de usuários LDAP é exibida.

3. Clique no grupo de usuários LDAP que deseja excluir.

4. Na parte superior da área de configurações exibida, clique em **Gerenciamento**→ **Excluir**.

5. Na janela de confirmação, clique em **Excluir**.

O grupo de usuários LDAP é excluído e não é mais exibido na tabela.

Ativar ou desativar a autenticação de dois fatores para todos os usuários

É possível ativar ou desativar a autenticação de dois fatores para todos os usuários. Se a autenticação de dois fatores for desativada para todos os usuários, não será possível ativá-la para usuários locais e LDAP ou grupos de usuários LDAP. A autenticação de dois fatores está desativada por padrão.

Para ativar ou desativar a autenticação de dois fatores para todos os usuários:

1. No menu, acesse a seção **Usuários**.

   A página de gerenciamento de usuários é exibida. A guia **Usuários**, selecionada por padrão, exibe a tabela de usuários.

2. Selecione a guia **Autenticação de dois fatores**.

3. Execute um dos seguintes:

   - Para ativar a autenticação de dois fatores para todos os usuários, marque a caixa de seleção **Autenticação de dois fatores para todos os usuários**. Todos os usuários devem concluir a autenticação de dois fatores na próxima vez que um usuário fizer login na interface da Web do orquestrador.

   - Para desativar a autenticação de dois fatores para todos os usuários, desmarque a caixa de seleção **Autenticação de dois fatores para todos os usuários**.

   Esta caixa de seleção é selecionada por padrão.

A autenticação de dois fatores é ativada ou desativada para todos os usuários.

Gerenciar solicitações de confirmação

Se ao criar ou editar um usuário, a caixa de seleção **Confirmação de solicitação obrigatória** tiver sido marcada, uma solicitação de confirmação é criada automaticamente para cada ação do usuário. É possível confirmar, negar ou excluir a solicitação de confirmação. Quando uma solicitação é confirmada, a ação correspondente é aplicada; solicitações de confirmação negadas são salvas na interface da Web do orquestrador.

Para confirmar, negar ou excluir uma solicitação de confirmação:

1. No menu, acesse a seção **Confirmação**.

   Uma tabela de solicitações de confirmação é exibida. As informações sobre solicitações de confirmação são exibidas nas seguintes colunas da tabela:

   - **Método** é o método de API usado para criar a solicitação de confirmação.

   - **URL** é a URL da API.

   - **Observação** é uma breve descrição da solicitação de confirmação.

   - **Usuário** é o nome do usuário cuja ação resultou na criação de uma solicitação de confirmação.

- **Cabeçalhos** são cabeçalhos de API.
- **Criado** é a data e hora em que a solicitação de confirmação foi criada.
- **Status** é o status da solicitação de confirmação:
  - **Confirmado**
  - **Negado**
  - **Erro**
  - **Aguardando confirmação**

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

2. Se necessário, execute uma das seguintes ações:
   - Para confirmar a solicitação, clique em **Permitir** ao lado dela.
   - Para negar a solicitação, clique em **Negar** ao lado dela.
   - Para excluir a solicitação, clique em **Excluir** ao lado dela.

   Para confirmar, negar ou excluir várias solicitações de confirmação ao mesmo tempo, marque as caixas de seleção ao lado das solicitações e selecione uma ação clicando no botão **Ação** na parte superior da tabela.

As solicitações de confirmação são confirmadas, negadas ou excluídas.

Gerenciar sessões de usuário

É possível fazer o seguinte com as sessões de usuário:

- Limitar a duração das sessões de usuário. Por padrão, se um usuário permanece ocioso por 3600 segundos (uma hora) após fazer login na interface da Web do orquestrador, a sessão do usuário é encerrada.
- Visualizar e, se necessário, encerrar as sessões de usuário ativas.

Para gerenciar sessões de usuário:

1. No menu, acesse a seção **Sistema**.

   Por padrão, é selecionada a guia **Monitoramento**, que exibe as configurações de conexão do servidor Zabbix.

2. Selecione a guia **Sessões de usuário**.

   Uma tabela de sessões de usuário é exibida. As informações sobre as sessões do usuário são exibidas nas seguintes colunas da tabela:
   - **Endereço IP** é o endereço IP do usuário.
   - **Agente do usuário** são informações sobre o navegador e o sistema operacional do usuário.
   - **Data** é a data de início da sessão do usuário.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

3. Se necessário, execute uma das seguintes ações:

   - Para limitar a duração das sessões de usuário, no campo **Quando ocioso, encerrar sessão após (s)**, insira o tempo em segundos após o qual uma sessão de usuário ociosa deve ser encerrada. Intervalo de valores: 60 a 86.400. O valor padrão é `3600`.

   - Para encerrar uma sessão de usuário específica, clique em **Encerrar sessão** ao lado dela.

   - Para encerrar várias sessões de usuário, marque as caixas de seleção ao lado delas e, na parte superior da tabela, clique em **Ações** → **Encerrar sessão**.

4. Clique em **Salvar**.

Multilocação

O Kaspersky SD-WAN pode ser implementado para vários *locatários*, que podem ser clientes independentes, escritórios ou departamentos de sua organização. A solução implementada para um locatário é chamada de *instância SD-WAN*. Após implementar a solução, crie pelo menos um locatário e implemente uma instância SD-WAN para ele.

Ao criar um locatário, o locatário obtém seu próprio portal de autoatendimento para gerenciar a instância SD-WAN. Os locatários criados são isolados para que não possam acessar os portais de autoatendimento uns dos outros e suas redes IP podem se sobrepor. O número de locatários criados não deve exceder o número de locatários especificado na seção `externa` do arquivo de configuração ao implementar a solução.

Para implementar uma instância SD-WAN para um locatário, crie um modelo de instância SD-WAN. No modelo de instância SD-WAN, especifique as configurações básicas da instância SD-WAN, como qualidade de serviço e configurações do serviço de transporte. Também é necessário adicionar o locatário ao modelo de instância SD-WAN, para que as configurações do modelo sejam aplicadas à instância SD-WAN quando ela for implementada para esse locatário.

Se o locatário não tiver sido adicionado a nenhum modelo de instância SD-WAN, o **modelo de SD-WAN padrão** será usado ao implementar uma instância SD-WAN para ele. É possível designar um modelo de instância SD-WAN diferente como padrão.

Se as configurações especificadas no modelo de instância SD-WAN não corresponderem aos parâmetros reais da instância SD-WAN, a instância não será implementada para o locatário. Por exemplo, uma instância SD-WAN não é implementada se o número de nós do controlador especificado no modelo de instância SD-WAN não corresponder ao número real de nós do controlador da instância.

Após implementar a instância SD-WAN, é possível visualizar os resultados de monitoramento e as solicitações de serviço da instância, bem como configurar seus nós do controlador. Também é possível adicionar locatários a uma instância SD-WAN implementada para permitir que eles usem o controlador da instância. Isso evita a necessidade de implementar uma instância SD-WAN separada para cada locatário.

É possível agrupar instâncias SD-WAN em pools de instâncias SD-WAN para balanceamento de carga quando muitos CPEs são usados. É possível adicionar dispositivos CPE a um pool de instâncias SD-WAN. Caso um dispositivo CPE tenha sido adicionado a um pool de instâncias SD-WAN, o orquestrador selecionará automaticamente a instância SD-WAN com o menor número de dispositivos CPE e adicionará o dispositivo CPE a essa instância. Se as instâncias SD-WAN no pool tiverem o mesmo número de dispositivos CPE, o orquestrador adicionará o dispositivo CPE a uma instância SD-WAN selecionada aleatoriamente.

Cenário: implementar uma instância SD-WAN para um locatário

O cenário de implementação de uma instância SD-WAN para um locatário envolve as seguintes etapas:

1. **Criar um locatário**

   Crie o locatário para o qual deseja implementar uma instância SD-WAN.

2. **Criar um modelo de instância SD-WAN**

   Crie e configure um modelo de instância SD-WAN. Para obter detalhes sobre o gerenciamento de modelos de instância SD-WAN, consulte a seção Gerenciar modelos de instância SD-WAN. É possível usar o modelo de instância SD-WAN criado para implementar outras instâncias SD-WAN.

3. **Adicionar um locatário a um modelo de instância SD-WAN**

   Adicione o locatário ao modelo de instância SD-WAN para que as configurações do modelo sejam aplicadas à instância SD-WAN quando ela for implementada para esse locatário.

4. **Preparar máquinas virtuais ou servidores físicos para a implementação do controlador**

   Ao implementar o Kaspersky SD-WAN, você preparou máquinas virtuais ou servidores físicos para a implementação de todos os componentes da solução, incluindo o controlador.

   Caso não tenha preparado máquinas virtuais ou servidores físicos para o controlador, poderá especificá-los na seção `nodes` do arquivo de configuração e, em seguida, executar o comando de implementação da solução novamente. Ao executar o comando de implementação da solução novamente, as máquinas virtuais ou os servidores físicos ausentes são preparados. Os componentes da solução já implementados não são afetados.

5. **Preparar o pacote de PNF do controlador**

   Prepare o pacote de PNF do controlador da instância SD-WAN no dispositivo local:

   1. Extraia o arquivo de instalação e acesse um dos seguintes diretórios:

      - Para implementar um único nó do controlador, acesse o diretório pnfs/pnf_sdwan_ctl.
      - Para implementar três nós do controlador, acesse o diretório /pnfs/pnf_sdwan_ctl_3.
      - Para implementar cinco nós do controlador, acesse o diretório /pnfs/pnf_sdwan_ctl_5.

   2. Para alterar o descritor de PNF do controlador, acesse o diretório /src do arquivo de instalação extraído e edite o arquivo pnfd.xml.

   3. Crie o pacote de PNF executando o seguinte comando:

      ```
      make
      ```

   O pacote de PNF é colocado no diretório /build do arquivo de instalação extraído.

6. **Carregar o pacote de PNF do controlador para a interface da Web do orquestrador**

   Carregue o pacote de PNF do controlador da instância SD-WAN para a interface da Web do orquestrador.

7. **Configurar o PNF do controlador**

   Configure o PNF do controlador da instância SD-WAN:

   1. No menu, acesse a seção **Catálogo** e, no painel **Catálogo**, clique no PNF do controlador.

   2. Na área de configurações exibida, selecione a guia **Posicionamento do DC** e, no campo **Data center**, especifique o data center adicionado no qual deseja implementar o controlador.

   3. Selecione a guia **IP de gerenciamento** e especifique os endereços IP dos nós do controlador. Especifique endereços IP padrão ou virtuais de máquinas virtuais ou servidores físicos para a implementação do controlador especificado na seção `nodes` do arquivo de configuração ao implementar a solução.

8. **Atribuir o PNF do controlador ao locatário**

   Atribua o PNF do controlador da instância SD-WAN ao locatário.

9. **Fazer login no portal de autoatendimento do locatário**

   Faça login no portal de autoatendimento do locatário

10. **Criar um serviço de rede SD-WAN**

    Crie um serviço de rede SD-WAN. Ao criar o serviço de rede SD-WAN, adicione o PNF do controlador da instância SD-WAN à topologia e, em seguida, fazer o seguinte:

    1. Na topologia, clique no PNF do controlador.
    2. Na área de configurações exibida, selecione a guia **CA_certificates** e, no campo **Certificado CA**, insira o certificado raiz no formato PEM com o qual o certificado do orquestrador é assinado. Há suporte para certificados raiz independentes, bem como cadeias de certificados que consistem em um certificado raiz e vários certificados intermediários. Ao especificar uma cadeia de certificados, inicie cada certificado em uma nova linha.
    3. Selecione a guia **Orquestrador** e, no campo **IP da API do orquestrador**, insira o endereço IP de um dos nós do orquestrador. É necessário especificar um dos endereços IP padrão ou virtuais das máquinas virtuais ou dos servidores físicos para a implementação do orquestrador especificado na seção `nodes` do arquivo de configuração.
    4. Selecione as guias **CTL1–5** e insira as informações do nó do controlador:
       1. No campo **IP para conexão ORC**, insira o endereço IP do nó do controlador para conectar o orquestrador. É necessário especificar um dos endereços IP padrão ou virtuais das máquinas virtuais ou dos servidores físicos para a implementação do controlador especificado na seção `nodes` do arquivo de configuração.
       2. No campo **IP para conexões CPE**, insira o endereço IP do nó do controlador para conectar dispositivos CPE.
       3. No campo **PORTA para conexões CPE**, insira a porta TCP do nó do controlador para conectar dispositivos CPE.

11. **Implementar o serviço de rede SD-WAN**

    Implemente o serviço de rede SD-WAN.

A instância SD-WAN é implementada para o locatário, e o controlador da instância SD-WAN é exibido no portal do administrador e no portal de autoatendimento do locatário na seção **Infraestrutura**.

Se na etapa 10 deste cenário, tive sido especificado um certificado raiz errado:

1. Estabeleça uma conexão com a máquina virtual ou o servidor físico no qual o nó do controlador está implementado. Em conjunto com cada nó do controlador, o componente MOCKPNF é implementado automaticamente na máquina virtual ou servidor físico para garantir a segurança da configuração do contêiner Docker do nó do controlador.
2. Faça login na conta de usuário com acesso ao grupo do Docker e, em seguida, faça login no contêiner Docker do componente MOCKPNF executando o seguinte comando:

   ```
   docker exec -it mockpnf-<número do nó do controlador> /bin/ash
   ```

3. Execute o script `cleanup.sh`. É possível baixar o script a partir do diretório /pnfs/pnf_sdwan_ctl<número de nós do controlador>/scr/scripts do arquivo de instalação.

   É necessário concluir as etapas 2 e 3 para cada nó do controlador.

4. Repita a etapa 10 deste cenário com o certificado raiz correto.

Gerenciar locatários

É possível visualizar a tabela de locações na seção **Locatários**. As informações sobre as locações são exibidas nas seguintes colunas da tabela:

- **Nome**
- **Descrição**
- **ID da instância SD-WAN**
- **Status da instância SD-WAN**
- **VIMs**
- **UNIs**

Criar um locatário

O número de locatários criados não deve exceder o número de locatários especificado na seção `externa` do arquivo de configuração ao implementar a solução.

Para criar um locatário:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Comece a criar o locatário de uma das seguintes formas:

   - Para criar o primeiro locatário, em **Locatários**, no campo **Nome**, insira o nome do locatário.
   - Para criar o segundo locatário ou os subsequentes, na parte superior da seção **Locatários**, clique em **+ Locatário** e, no campo **Nome**, insira o nome do locatário.

3. Se necessário, na área relevante da parte inferior da página, insira uma breve descrição do locatário.

4. Clique no ícone de criar +.

O locatário é criado e exibido em **Locatários**.

Atribuir um usuário a um locatário

É possível atribuir um usuário a uma locação para permitir que o usuário faça login no portal de autoatendimento da locação e gerencie a instância SD-WAN que está implementada para a locação. Para atribuir um usuário a uma locação, é necessário primeiro atribuir a função de locação **Locatário**ao usuário ao criar ou editar o usuário. Você pode atribuir a um usuário a função **Locatário** para várias locações ou atribuir vários usuários com a função **Locatário** para uma locação.

Para atribuir usuários a uma locação:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Clique no nome da locação para a qual você deseja atribuir usuários ou selecione-a na tabela e clique no botão **Editar locatário**.

   Isso abre a área de configurações da locação.

3. Vá para a guia **Usuários** e ative o interruptor de alternância **Usar** para um ou mais usuários que você deseja atribuir a uma locação.

   Se você quiser atribuir todos os grupos na tabela a uma locação, clique no botão **Usar tudo**.

Os usuários são atribuídos à locação. A locação para a qual você atribuiu usuários é exibida na seção **Usuários** na tabela de usuários na coluna **Locatário**.

Atribuir um grupo de usuários LDAP a um locatário

Você pode atribuir grupos LDAP a uma locação para permitir que os usuários do grupo façam login no portal de autoatendimento da locação e gerenciem a instância SD-WAN que está implementada para a locação. Para atribuir um grupo de usuários LDAP a uma locação, você deve primeiro atribuir a função **Locatário** para o grupo de usuários LDAP ao criar ou editar o grupo de usuários LDAP. Você pode atribuir um grupo de usuários LDAP com a função **Locatário** para várias locações ou atribuir vários grupos de usuários LDAP com a função **Locatário** para uma locação.

Para atribuir um grupo de usuários LDAP a um locatário:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Clique no nome da locação para a qual você deseja atribuir um grupo de usuários LDAP ou selecione-o na tabela e clique no botão **Editar locatário**.

   Isso abre a área de configurações da locação.

3. Vá para a guia **Grupos de usuários** e ative o interruptor de alternância **Usar** para um ou mais grupos de usuários LDAP que você deseja atribuir a uma locação.

   Se você quiser atribuir todos os grupos na tabela a uma locação, clique no botão **Usar tudo**.

Os grupos de usuários LDAP são atribuídos à locação. A locação para a qual você atribuiu grupos de usuários LDAP é exibida na seção **Usuários** →**Grupos** na tabela de usuários na coluna **Locatário**.

Atribuir recursos de computação a um locatário

É possível atribuir recursos de computação a um locatário para configurar o desempenho da instância SD-WAN que deseja implementar para ele. A quantidade de recursos de computação disponíveis é determinada durante a implementação da solução.

Para atribuir recursos de computação a um locatário:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Em **Locatários**, selecione o locatário ao qual deseja atribuir recursos de computação.

3. Na parte superior da seção **Recursos**, clique no ícone de configurações ⚙.

4. Clique no ícone de redimensionamento ∞ ao lado de um dos seguintes recursos de computação:

   - **CPU** — núcleos de CPU virtuais
   - **RAM** — RAM
   - **Disco** — espaço em disco

5. No campo exibido, insira a quantidade de recurso de computação que deseja atribuir ao locatário.

6. Clique no ícone de salvar ✓.

A quantidade de recursos de computação especificada é atribuída ao locatário.

Atribuir componentes do serviço de rede a um locatário

É possível atribuir componentes do serviço de rede a um locatário para permitir que ele os use para gerenciar serviços de rede.

Para atribuir componentes do serviço de rede a um locatário:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Em **Locatários**, selecione o locatário ao qual deseja atribuir componentes do serviço de rede.

3. Em **Catálogo**, marque as caixas de seleção ao lado dos componentes do serviço de rede que deseja atribuir ao locatário.

Os componentes do serviço de rede são atribuídos ao locatário e exibidos no portal de autoatendimento do locatário na seção **Catálogo**.

Atribuir um VIM a um locatário

Você pode atribuir um ou mais VIMs a uma locação para permitir que ela use esses VIMs para gerenciar funções de rede virtual na infraestrutura virtual.

Para atribuir um VIM a um locatário:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Em **Locatários**, selecione a locação para a qual você deseja atribuir os VIMs e clique no botão **+ Editar VIMs**.

   Isso abre a área de configurações do VIM para a locação.

3. Na guia **Lista**, na tabela, ative o interruptor de alternância **Usar** para um ou mais VIMs que você deseja atribuir a uma locação.

4. Você pode filtrar a lista de VIMs usando as listas suspensas **Domínio** e **Data center** ao selecionar o domínio criado e o data center adicionado no qual você implementou os VIMs.

Os VIMs são atribuídos à locação e exibidos na tabela de locações na coluna **VIMs**.

Fazer login no portal de autoatendimento do locatário

Para fazer login no portal de autoatendimento do locatário:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Em **Locatários**, selecione no portal de autoatendimento de qual locatário deseja fazer login.

3. Clique em **Conectar como locatário**.

Isso abre o portal de autoatendimento do locatário em uma nova guia do navegador. Você fez login no portal de autoatendimento.

Editar um locatário

Para editar um locatário:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Na seção **Locatários**, clique no ícone de configurações → **Editar** ao lado do locatário que deseja editar.

3. Se necessário, edite o nome e/ou a descrição do locatário.

4. Clique no ícone de salvar ✓.

O locatário é modificado e atualizado em **Locatários**.

Excluir um locatário

Ao excluir um locatário, a instância SD-WAN implementada para ele é excluída automaticamente. Ao mesmo tempo, todos os objetos criados no locatário, como zonas e modelos de firewall, são salvos no portal do administrador.

Locatários excluídos não podem ser restaurados.

Para excluir um locatário:

1. No menu, acesse a seção **Locatários**.

   A página de gerenciamento de locatários é exibida.

2. Na seção **Locatários**, clique no ícone de configurações ⚙ → **Excluir** ao lado do locatário que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

O locatário é excluído e não é mais exibido em **Locatários**.

Gerenciar modelos de instância SD-WAN

É possível visualizar a tabela de modelos de instância SD-WAN na seção **SD-WAN** → **Modelos de instância SD-WAN**. **O modelo de SD-WAN padrão** é o modelo de instância SD-WAN criado por padrão. As informações sobre modelos de instância SD-WAN são exibidas nas seguintes colunas da tabela:

- **ID** é o ID do modelo de instância SD-WAN.
- **Nome** é o nome do modelo de instância SD-WAN.
- **Usado** especifica se o modelo de instância SD-WAN está sendo usado por instâncias SD-WAN:
  - **Sim**.
  - **Não**.
- **Atualizado** é a data e hora em que as configurações do modelos de instância SD-WAN foram modificadas pela última vez.
- **Usuário** é o nome do usuário que criou o modelo de instância SD-WAN.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

É possível gerenciar as configurações do modelo de instância SD-WAN nas seguintes guias:

- **Informações** contém informações básicas sobre o modelo de instância SD-WAN. É possível editar o nome do modelo de SD-WAN no campo **Nome**.
- **Classes de tráfego** contém configurações de classes de tráfego.
- **Classificadores de tráfego** contém configurações de classificadores de tráfego.
- **Regras de QoS** contém configurações de regras de qualidade de serviço.
- **Serviços de transporte** contém configurações de serviços de transporte.
- **Locatários** contém locatários que foram adicionados ao modelo de instância SD-WAN.
- **Alta disponibilidade**é o número de nós do controlador da instância SD-WAN.
- **Estratégias de serviços/transporte** é a estratégia de transporte usada na instância SD-WAN.

Criar um modelo de instância SD-WAN

Para criar um modelo de instância SD-WAN:

1. No menu, acesse a seção **SD-WAN** → **Modelos de instância SD-WAN**.
   Uma tabela de modelos de instância SD-WAN é exibida.
2. Na parte superior da página, clique em **+ Adicionar**.
3. Na janela aberta, insira o nome do modelo de instância SD-WAN.
4. Clique em **Criar**.

   O modelo de instância SD-WAN é criado e exibido na tabela.

É necessário configurar o modelo de instância SD-WAN criado. No modelo de instância SD-WAN, especifique as configurações básicas da instância SD-WAN, como qualidade de serviço e configurações do serviço de transporte. Também é necessário adicionar o locatário ao modelo de instância SD-WAN, para que as configurações do modelo sejam aplicadas à instância SD-WAN quando ela for implementada para esse locatário. Para obter detalhes sobre o gerenciamento de modelos de instância SD-WAN, consulte a seção Gerenciar modelos de instância SD-WAN.

Definir o modelo de instância SD-WAN padrão

Se o locatário não tiver sido adicionado a nenhum modelo de instância SD-WAN, o **modelo de SD-WAN padrão** será usado ao implementar uma instância SD-WAN para ele. É possível designar um modelo de instância SD-WAN diferente como padrão.

Para definir o modelo de instância SD-WAN padrão:

1. No menu, acesse a seção **SD-WAN** → **Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN que deseja tornar o modelo padrão.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Na parte superior da área de configurações, em **Ações**, clique em **Definir como modelo padrão**.

O modelo de instância SD-WAN se torna o modelo padrão.

Selecionar o número de nós do controlador para uma instância SD-WAN

Uma instância SD-WAN não é implementada se o número de nós do controlador especificado no modelo de instância SD-WAN não corresponder ao número real de nós do controlador da instância.

Para selecionar o número de nós do controlador da instância SD-WAN:

1. No menu, acesse a seção **SD-WAN** → **Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN para o qual deseja selecionar o número de nós do controlador.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Selecione a guia **Alta disponibilidade**.

4. Selecione o número de nós do controlador

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Adicionar um locatário a um modelo de instância SD-WAN

É necessário adicionar o locatário ao modelo de instância SD-WAN para que as configurações do modelo sejam aplicadas a ela quando a instância SD-WAN for implementada para esse locatário.

Para adicionar um locatário a um modelo de instância SD-WAN:

1. No menu, acesse a seção **SD-WAN** → **Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN ao qual deseja adicionar um locatário.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Selecione a guia **Locatários**.

   Uma tabela de locatários é exibida.

4. Clique em **+ Locatário**.

5. Na janela aberta, selecione o locatário criado que deseja adicionar ao modelo de instância SD-WAN.

6. Clique em **Adicionar**.

   O locatário é adicionado ao modelo de instância SD-WAN e exibido na tabela.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Remover um locatário de um modelo de instância SD-WAN

É possível remover um locatário de um modelo de instância SD-WAN; ao fazer isso, o modelo de instância SD-WAN não será usado na implementação da instância SD-WAN para o locatário.

Para remover um locatário de um modelo de instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN do qual deseja remover um locatário.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Selecione a guia **Locatários**.

   Uma tabela de locatários é exibida.

4. Clique em **Excluir** ao lado do locatário que deseja remover do modelo de instância SD-WAN.

   O locatário é removido do modelo de instância SD-WAN e não é mais exibido na tabela.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Excluir um modelo de instância SD-WAN

Não é possível excluir o modelo de instância SD-WAN padrão.

Os modelos de instância SD-WAN excluídos não podem ser restaurados.

Para excluir um modelo de instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN que deseja excluir.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

O modelo de instância SD-WAN é excluído e não é mais exibido na tabela.

Gerenciar instâncias SD-WAN

É possível visualizar a tabela de instâncias SD-WAN na seção **SD-WAN → Instâncias SD-WAN**. As informações sobre instâncias SD-WAN são exibidas nas seguintes colunas da tabela:

- **ID** é o ID da instância SD-WAN.
- **Locatário** é o locatário para o qual a instância SD-WAN é implementada.
- **Status** é o status da instância SD-WAN:
  - **OK** significa que a instância SD-WAN está operando normalmente.
  - **Controlador ausente** significa que a instância SD-WAN não tem um controlador.
  - **Erro** significa que ocorreu um erro durante a operação da instância SD-WAN.
  - **Excluindo** significa que a instância SD-WAN está em processo de exclusão.
  - **Excluído** significa que a instância SD-WAN foi excluída.
- **CPEs** é o número de dispositivos CPE que foram adicionados à instância SD-WAN.
- **Controladores** são endereços IP e números de porta dos controladores da instância SD-WAN.
- **DC** é o data center no qual a instância SD-WAN é implementada.
- **VIM** é o VIM da instância SD-WAN.
- **Criado** é a data e hora em que a instância SD-WAN foi implementada.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

É possível gerenciar as configurações da instância SD-WAN nas seguintes guias:

- **Configuração** contém informações básicas sobre a instância SD-WAN e as configurações dos nós do controlador da instância. É possível inserir uma breve descrição da instância SD-WAN no campo **Descrição**.
- **Monitoramento** contém os resultados de monitoramento da instância SD-WAN.
- **Solicitações de serviço** contém solicitações de serviço da instância SD-WAN.
- **Autoatendimento do locatário** contém locatários que foram adicionados à instância SD-WAN.

Configurar os nós do controlador de uma instância SD-WAN

Ao configurar os nós do controlador da instância SD-WAN, é possível alterar os endereços IP e números de porta TCP. Isso altera automaticamente os endereços IP e os números de porta TCP dos nós do controlador em todos os dispositivos CPE adicionados à instância SD-WAN. Se as interfaces SD-WAN do tipo WAN do dispositivo CPE estiverem conectadas a redes diferentes, por exemplo, a Internet e uma rede MPLS privada, é possível alterar os endereços IP e os números de porta TCP dos nós do controlador em interfaces SD-WAN do tipo WAN individuais ao criar ou editar interfaces SD-WAN do tipo WAN. Os endereços IP e os números de porta TCP especificados em uma interface SD-WAN do tipo WAN individual têm precedência sobre os endereços IP e os números de porta TCP especificados ao configurar os nós do controlador da instância SD-WAN.

Caso vários nós do controlador tenham sido implementados ao implementar a instância SD-WAN, é possível especificar qual deles é o nó árbitro durante a configuração dos nós do controlador da instância SD-WAN. Quando um nó árbitro é especificado na interface da Web do orquestrador, os dispositivos CPE não estabelecem sessões de gerenciamento com esse nó do controlador, reduzindo a carga nos dispositivos CPE.

Após configurar os nós do controlador da instância SD-WAN, para aplicar as alterações, reinicie os dispositivos CPE já registrados.

Para configurar os nós do controlador de uma instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Instâncias SD-WAN**.

   Uma tabela de instâncias SD-WAN é exibida.

2. Clique na instância SD-WAN cujos nós do controlador deseja configurar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configuração**, que exibe informações gerais sobre a instância SD-WAN.

3. Se necessário, execute uma das seguintes ações:

   - Para alterar o endereço IP de um nó do controlador, no campo **Endereço IP**, insira um endereço IPv4. O número de campos corresponde ao número de nós do controlador.

   - Para alterar o número da porta TCP de um nó do controlador, no campo **Porta**, insira o número da porta base. Intervalo de valores: 1 a 65.535. O valor padrão é `6653`. O número de campos corresponde ao número de nós do controlador.

     Com a porta base do nó do controlador, as portas com os próximos três números consecutivos são especificadas automaticamente. Por exemplo, ao inserir `6653` como o número da porta base, as portas 6654, 6655 e 6656 serão especificadas automaticamente.

   - Para especificar um nó árbitro, marque a caixa de seleção **Árbitro** ao lado do nó do controlador. Não é possível especificar um nó árbitro se apenas um nó do controlador tiver sido implementado ao implementar a instância SD-WAN.

4. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da instância SD-WAN.

Visualizar o uso de uma instância SD-WAN

Se necessário, é possível verificar que dispositivos CPE foram adicionados à instância SD-WAN.

Para ver se uma instância SD-WAN está em uso:

1. No menu, acesse a seção **SD-WAN → Instâncias SD-WAN**.

   Uma tabela de instâncias SD-WAN é exibida.

2. Clique na instância SD-WAN cujas informações de uso deseja visualizar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⩓. Por padrão, é selecionada a guia **Configuração**, que exibe informações gerais sobre a instância SD-WAN.

3. Na parte superior da área de configurações, em **Ações**, clique em **Mostrar CPEs associados**.

Isso abre a seção **CPE**, que exibe uma tabela de dispositivos CPE adicionados à instância SD-WAN.

Visualizar a topologia de uma instância SD-WAN

Para visualizar a topologia de uma instância SD-WAN:

1. Faça login no portal de autoatendimento do locatário para o qual a instância SD-WAN está implementada.

2. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

3. Clique em **Gerenciamento → Configurações de implementação** ao lado do controlador.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

4. Vá para a seção **Topologia**.

   A topologia da instância SD-WAN é exibida.

5. Se necessário, marque as seguintes caixas de seleção:

   - Marque a caixa de seleção **Utilização do link** para exibir a utilização dos links. O nível de utilização do link é representado pelas seguintes cores:

     - Verde — Baixa utilização do link.
     - Amarelo — Média utilização do link.
     - Vermelho — Alta utilização do link.

   - Marque a caixa de seleção **Segmentos** e, na lista suspensa **Switches de segmento**, selecione dois dispositivos CPE para exibir todos os links link entre eles.
   - Marque a caixa de seleção **Nome** para exibir os nomes dos dispositivos CPE.
   - Marque a caixa de seleção **Endereço IP** para exibir os endereços IP dos dispositivos CPE.

   Por padrão, todas as caixas de seleção estão desmarcadas.

Adicionar um locatário a uma instância SD-WAN

Para usar o controlador de uma única instância SD-WAN para vários locatários, é necessário adicionar locatários à instância SD-WAN. Usar um único controlador de instância SD-WAN para vários locatários elimina a necessidade de implementar uma instância SD-WAN separada para cada locatário.

Para adicionar um locatário a uma instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Instâncias SD-WAN**.

   Uma tabela de instâncias SD-WAN é exibida.

2. Clique na instância SD-WAN à qual deseja adicionar um locatário.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configuração**, que exibe informações gerais sobre a instância SD-WAN.

3. Selecione a guia **Autoatendimento do locatário**.

   Uma tabela de locatários é exibida.

4. Clique em **+ Adicionar**.

5. Na janela aberta, selecione o locatário criado que deseja adicionar à instância SD-WAN.

6. No campo **CPEs máximos**, insira o número máximo de dispositivos CPE disponíveis para o locatário.

7. Clique em **Adicionar**.

O locatário é adicionado à instância SD-WAN e exibido na tabela.

Remover um locatário de uma instância SD-WAN

É possível remover um locatário adicionado a uma instância SD-WAN para impedir que ele use o controlador da instância SD-WAN.

Para remover um locatário de uma instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Instâncias SD-WAN**.

   Uma tabela de instâncias SD-WAN é exibida.

2. Clique na instância SD-WAN da qual deseja remover um locatário.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configuração**, que exibe informações gerais sobre a instância SD-WAN.

3. Selecione a guia **Autoatendimento do locatário**.

   Uma tabela de locatários é exibida.

4. Clique em **Excluir** ao lado do locatário que deseja remover da instância SD-WAN.

5. Na janela de confirmação, clique em **Excluir**.

O locatário é excluído da instância SD-WAN e não é mais exibido na tabela.

Excluir uma instância SD-WAN

Ao excluir uma instância SD-WAN, os dispositivos CPE que foram adicionados a ela e o serviço de rede SD-WAN implementado para a instância SD-WAN também são automaticamente excluídos. No entanto, o locatário para o qual a instância SD-WAN foi implementada não é excluído. Uma forma alternativa de excluir uma instância SD-WAN é excluir o serviço de rede SD-WAN.

As instâncias SD-WAN excluídas não podem ser restauradas.

Para excluir uma instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Instâncias SD-WAN**.

   Uma tabela de instâncias SD-WAN é exibida.

2. Clique na instância SD-WAN que deseja excluir.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configuração**, que exibe informações gerais sobre a instância SD-WAN.

3. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

A instância SD-WAN é excluída e não é mais exibida na tabela.

Gerenciar pools de instâncias SD-WAN

É possível visualizar a tabela de pools de instâncias SD-WAN na seção **SD-WAN → Pools de instância SD-WAN**. As informações sobre pools de instâncias SD-WAN são exibidas nas seguintes colunas da tabela:

- **ID** é o ID do pool de instâncias SD-WAN.
- **Nome** é o nome do pool de instâncias SD-WAN.
- **Número de instâncias** é o número de instâncias SD-WAN no pool.
- **CPEs** é o número de dispositivos CPE que foram adicionados às instâncias SD-WAN.
- **Criado** é a data e hora em que o pool de instâncias SD-WAN foi criado.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

É possível gerenciar as configurações do pool de instâncias SD-WAN nas seguintes guias:

- **Informações** contém informações básicas sobre o pool de instâncias SD-WAN. É possível renomear o pool de instâncias SD-WAN no campo **Nome** e inserir uma breve descrição no campo **Descrição**.
- **Instâncias SD-WAN** contém instâncias SD-WAN que foram adicionadas ao pool de instâncias SD-WAN.

Criar um pool de instâncias SD-WAN

Para criar um pool de instâncias SD-WAN:

1. No menu, acesse a seção **SD-WAN → Pools de instância SD-WAN**.

   Uma tabela de pools de instâncias SD-WAN é exibida.

2. Na parte superior da página, clique em **+ Pool de instância SD-WAN**.
3. Na janela aberta, insira o nome do pool de instâncias SD-WAN.
4. Clique em **Criar**.

   O pool de instâncias SD-WAN é criado e exibido na tabela.

É necessário adicionar instâncias SD-WAN ao pool de instâncias SD-WAN criado.

Adicionar uma instância SD-WAN a um pool de instâncias SD-WAN

Para adicionar uma instância SD-WAN a um pool de instâncias SD-WAN:

1. No menu, acesse a seção **SD-WAN → Pools de instância SD-WAN**.

   Uma tabela de pools de instâncias SD-WAN é exibida.

2. Clique no pool de instâncias SD-WAN ao qual deseja adicionar uma instância SD-WAN.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o pool de instâncias SD-WAN.

3. Selecione a guia **Instâncias SD-WAN**.

   Uma tabela de instâncias SD-WAN é exibida.

4. Clique em **+ Adicionar**.

5. Na janela aberta, selecione a instância SD-WAN implementada que deseja adicionar ao pool de instâncias SD-WAN.

6. Clique em **Adicionar**.

   A instância SD-WAN é adicionada ao pool de instâncias SD-WAN e exibida na tabela.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do pool de instâncias SD-WAN.

Caso esteja adicionando um dispositivo CPE ao pool de instâncias SD-WAN, poderá adicionar esse dispositivo à instância SD-WAN adicionada ao pool. Isso acontece se o menor número de dispositivos CPE tiver sido adicionado à instância SD-WAN em comparação com as outras instâncias SD-WAN no pool de instâncias SD-WAN.

Remover uma instância SD-WAN de um pool de instâncias SD-WAN

Para remover uma instância SD-WAN de um pool de instâncias SD-WAN:

1. No menu, acesse a seção **SD-WAN → Pools de instância SD-WAN**.

   Uma tabela de pools de instâncias SD-WAN é exibida.

2. Clique no pool de instâncias SD-WAN do qual deseja remover uma instância SD-WAN.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o pool de instâncias SD-WAN.

3. Selecione a guia **Instâncias SD-WAN**.

   Uma tabela de instâncias SD-WAN é exibida.

4. Clique em **Excluir** ao lado da instância SD-WAN que deseja remover do pool de instâncias SD-WAN.

   A instância SD-WAN é removida do pool de instâncias SD-WAN e não é mais exibida na tabela.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do pool de instâncias SD-WAN.

Excluir um pool de instâncias SD-WAN

Ao excluir um pool de instâncias SD-WAN, todos os dispositivos CPE adicionados a esse pool são automaticamente excluídos. Isso não exclui as instâncias SD-WAN.

Os pools de instâncias SD-WAN excluídos não podem ser restaurados.

Para excluir um pool de instâncias SD-WAN:

1. No menu, acesse a seção **SD-WAN → Pools de instância SD-WAN**.

   Uma tabela de pools de instâncias SD-WAN é exibida.

2. Clique no pool de instâncias SD-WAN que deseja excluir.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o pool de instâncias SD-WAN.

3. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

O pool de instâncias SD-WAN é excluído e não é mais exibido na tabela.

Gerenciar dispositivos CPE

Os dispositivos CPE retransmitem o tráfego entre locais e clientes de sua organização, além de terem acesso direto à Internet (DIA) sem retransmitir o tráfego para o escritório central. Por padrão, para construir a rede SD-WAN, um switch virtual OpenFlow (switch virtual; vSwitch) é instalado nos dispositivos CPE. É possível usar os seguintes tipos de dispositivos CPE:

- Dispositivos CPE do modelo KESR (Kaspersky SD-WAN Edge Service Router) adquiridos da Kaspersky.
- Dispositivos CPE virtuais (dispositivos vCPE) implementados em máquinas virtuais. Ao usar dispositivos vCPE, certifique-se de que as máquinas virtuais atendam aos requisitos de hardware e software.
- Dispositivos CPE universais (dispositivos uCPE) com suporte à implementação de funções de rede virtual e VIM.

Para gerenciar dispositivos CPE, é necessário registrá-los.

É possível usar a *autenticação de dois fatores* para registrar o dispositivo CPE com segurança. Quando a autenticação de dois fatores está ativada, um token (chave de segurança) é registrado no banco de dados do orquestrador; esse token deve então ser colocado no dispositivo CPE ao registrá-lo usando a tecnologia Zero Touch Provisioning. O registro será bem-sucedido se, quando o dispositivo CPE estabelecer uma conexão automática com o orquestrador, o token no dispositivo corresponder ao token de CPE no banco de dados do orquestrador.

Para a configuração centralizada de dispositivos CPE, é possível usar modelos de CPE. Para evitar a configuração de cada dispositivo CPE individualmente, especifique as configurações no modelo de CPE e aplique o modelo de CPE aos dispositivos CPE ao adicionar ou registrar dispositivos CPE manualmente. Ao editar uma configuração em um modelo de CPE, a configuração é automaticamente modificada em todos os dispositivos CPE que estiverem usando o modelo. Ao editar uma configuração no dispositivo CPE, essa configuração se torna independente do modelo de CPE e, caso seja modificada no modelo de CPE, permanece inalterada no dispositivo CPE.

> Determinadas configurações de dispositivo CPE só podem ser especificadas em um modelo de CPE; por exemplo, o número da porta para estabelecer a conexão com o orquestrador.

Ao remover um dispositivo CPE da interface da Web do orquestrador, as configurações básicas são mantidas no dispositivo CPE. É possível registrar o dispositivo CPE novamente. Ao registrar um dispositivo CPE novamente, não é possível usar a autenticação de dois fatores.

Ao adicionar e registrar um dispositivo CPE, é possível selecionar se deseja que o dispositivo CPE seja ativado automaticamente após o registro. Quando um dispositivo CPE é ativado, o modelo de CPE é aplicado a ele e o dispositivo fica disponível para retransmitir o tráfego.

Para redefinir o dispositivo CPE para os padrões de fábrica sem removê-lo do orquestrador, pressione o botão Reset físico no dispositivo. Para isso, pressione e segure o botão por 10 segundos. Essa funcionalidade está disponível para os modelos KESR M1, M2 e M3.

Sobre a interação do dispositivo CPE com o orquestrador

Após o registro, o dispositivo CPE envia solicitações de API REST ao orquestrador para obter tarefas com um período especificado ao configurar a conexão do dispositivo CPE com orquestrador e controlador. *Tarefas* são ações que os usuários executam com o dispositivo CPE, como reiniciar o dispositivo CPE e atualizar o firmware. As solicitações da API REST são necessárias para obter tarefas que não estão associadas ao switch virtual do dispositivo CPE.

Para visualizar a tabela de tarefas executadas pelo orquestrador em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu e clique no dispositivo CPE. As informações sobre as tarefas são exibidas nas seguintes colunas da tabela:

- **Tipo** é o tipo de tarefa.
- **Status** é o status da tarefa:
  - **Aguarde** significa que a tarefa é salva no banco de dados do orquestrador e está aguardando para ser recebida pelo dispositivo CPE.
  - **Executando** significa que a tarefa está em execução.
  - **Concluída** significa que a tarefa foi concluída com êxito.
  - **Erro** significa que ocorreu um erro durante a execução da tarefa.
- **Última atualização** é a data e hora da última atualização da tarefa.

O orquestrador executa tarefas no dispositivo CPE da seguinte maneira:

1. Você executa uma tarefa no dispositivo CPE, como modificar as configurações de BGP, usando a interface da Web do orquestrador.
2. O orquestrador salva a tarefa no banco de dados. Na tabela, a tarefa é exibida com o status **Aguarde**.
3. O dispositivo CPE recebe a tarefa quando envia uma solicitação de API REST ao orquestrador. Na tabela, a tarefa é exibida com o status **Executando**.
4. Se a tarefa for concluída com êxito, o dispositivo CPE relata isso ao orquestrador. Na tabela, a tarefa é exibida com o status **Concluída**.

   Se a tarefa falhar, ela é exibida na tabela com o status**Erro**.

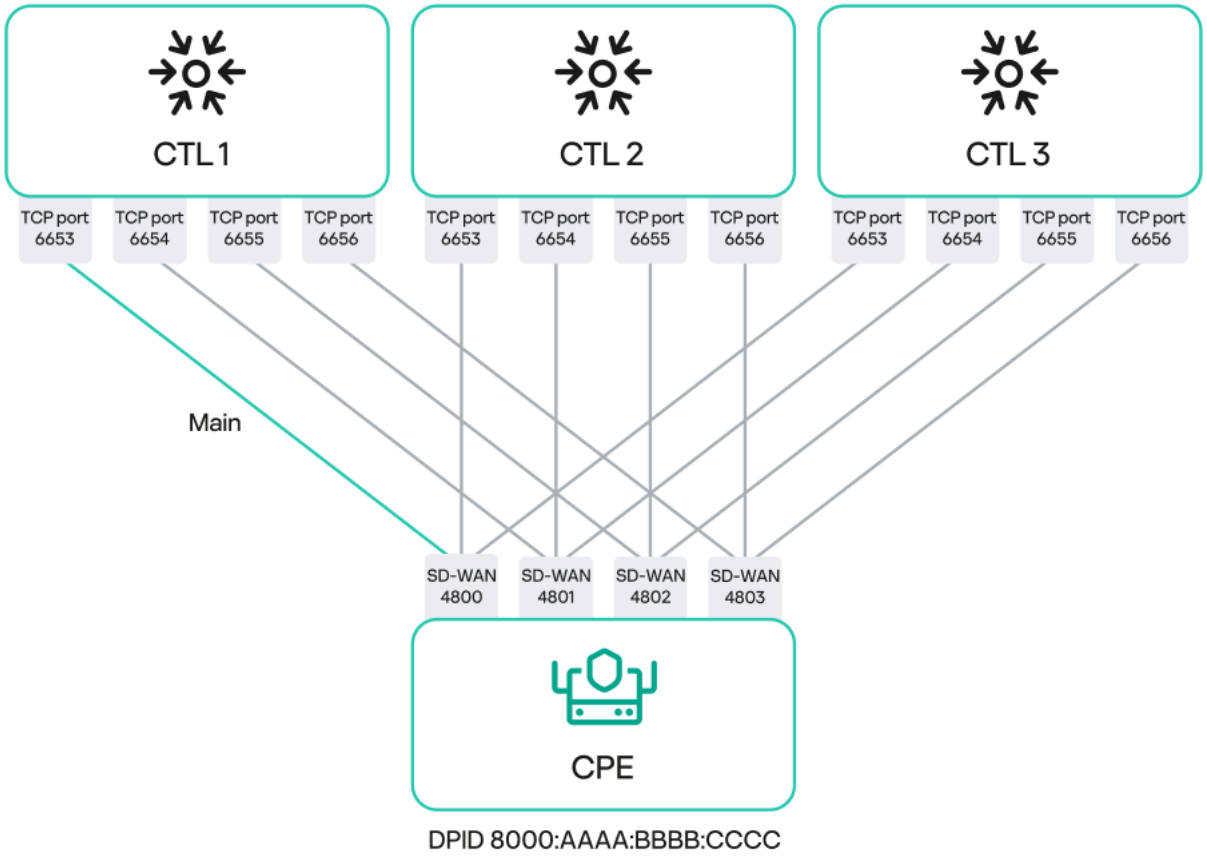
Antes de executar a tarefa, as configurações atuais no dispositivo CPE são salvas. Se o dispositivo CPE não puder enviar uma mensagem de confirmação ao orquestrador após a conclusão bem-sucedida da tarefa, após três tentativas, as configurações anteriores serão restauradas no dispositivo CPE e a tabela exibirá a tarefa com o status **Erro**.

Sobre a interação do dispositivo CPE com o controlador

Depois que o dispositivo CPE é registrado, são estabelecidas *sessões de gerenciamento* entre suas interfaces SD-WAN do tipo WAN e as portas TCP dos nós do controlador. Uma das sessões de gerenciamento é a sessão principal e as outras ficam no modo de espera. A sessão de gerenciamento principal é usada para transmitir tarefas relacionadas ao gerenciamento do switch virtual do dispositivo CPE, como modificar configurações de caminho. Se a sessão de gerenciamento principal for encerrada, uma nova sessão de gerenciamento principal é escolhida aleatoriamente a partir das sessões de gerenciamento estabelecidas anteriormente.

As sessões de gerenciamento são estabelecidas combinando os números de portas OpenFlow referenciados por interfaces SD-WAN do tipo WAN com os números de porta TCP dos nós do controlador, com base em sua ordem. Por exemplo, na figura abaixo, o dispositivo CPE tem quatro interfaces SD-WAN que fazem referência às portas OpenFlow 4800, 4801, 4802 e 4803. Os nós do controlador CTL 1–3 têm portas TCP 6653, 6654, 6655, 6656. Nesse caso, as sessões de gerenciamento são estabelecidas da seguinte forma:

- SD-WAN 4800 → 6653
- SD-WAN 4801 → 6654
- SD-WAN 4802 → 6655
- SD-WAN 4803 → 6656



Sessões de gerenciamento entre um dispositivo CPE e três nós do controlador

As sessões de gerenciamento podem ser configuradas durante a configuração da conexão do dispositivo CPE com orquestrador e controlador. Por exemplo, é possível selecionar uma interface SD-WAN do tipo WAN para priorizá-la com o objetivo de estabelecer a sessão de gerenciamento principal; também é possível ativar ou desativar a criptografia para sessões de gerenciamento.

É possível alterar os endereços IP e os números de porta TCP dos nós do controlador ao configurar os nós do controlador de uma instância SD-WAN. Isso altera automaticamente os endereços IP e os números de porta TCP dos nós do controlador em todos os dispositivos CPE adicionados à instância SD-WAN. Se as interfaces SD-WAN do tipo WAN do dispositivo CPE estiverem conectadas a redes diferentes, por exemplo, a Internet e uma rede MPLS privada, é possível alterar os endereços IP e os números de porta TCP dos nós do controlador em interfaces SD-WAN do tipo WAN individuais ao criar ou editar interfaces SD-WAN do tipo WAN. Os endereços IP e os números de porta TCP especificados em uma interface SD-WAN do tipo WAN individual têm precedência sobre os endereços IP e os números de porta TCP especificados ao configurar os nós do controlador da instância SD-WAN.

Para visualizar a tabela de dispositivos CPE com informações sobre sessões de gerenciamento, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador e vá para a seção **Switches**. As informações sobre sessões de gerenciamento são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do dispositivo CPE.
- **Ordem** é o número de sequência do dispositivo CPE. O menor número é atribuído ao dispositivo CPE que estabelece conexão com o controlador primeiro.
- **Status** é o status do dispositivo CPE em relação ao controlador:
  - **Ativo** significa que o dispositivo CPE pode ser usado para retransmitir tráfego.
  - **Inativo** significa que o dispositivo CPE não pode ser usado para retransmitir tráfego.
- **Conexão** é o status da conexão do dispositivo CPE ao controlador:
  - **Conectado** significa que as sessões de gerenciamento são estabelecidas entre o dispositivo CPE e os nós do controlador.
  - **Desconectado** significa que nenhuma sessão de gerenciamento é estabelecida entre o dispositivo CPE e os nós do controlador.
- **MAC** é o endereço MAC do dispositivo CPE.
- **Interface** são interfaces SD-WAN do tipo WAN a partir das quais as sessões de gerenciamento são estabelecidas.
- **Sessão principal** é a interface SD-WAN do tipo WAN a partir da qual a sessão de gerenciamento principal é estabelecida:
  - **Sim**.
  - **Não**.
- **Endereço IP** é o endereço IP que a interface SD-WAN do tipo WAN usou para estabelecer a sessão de gerenciamento.
- **Porta** é a porta TCP que a interface SD-WAN do tipo WAN usou para estabelecer a sessão de gerenciamento.
- **Criado** é a data e hora em que o dispositivo CPE foi registrado.
- **Localização** é o endereço do local do dispositivo CPE.

- **Latência (ms)** é a latência em milissegundos da sessão de gerenciamento.
- **Descrição** é uma breve descrição do dispositivo CPE.

Credenciais padrão dos dispositivos CPE KESR

Todos os dispositivos CPE do modelo KESR (Kaspersky SD-WAN Edge Service Router) têm as mesmas credenciais padrão:

- Nome do usuário: `root`
- Senha: `123-qwe`

É necessário inserir essas credenciais para estabelecer uma conexão com um dispositivo CPE KESR não registrado por meio de SSH ou para estabelecer uma sessão de console com ele. Após o registro, a senha padrão do dispositivo CPE é alterada automaticamente. É possível visualizar a senha do dispositivo CPE na interface da Web do orquestrador.

Verificação de integridade

Essa função permite verificar automática ou manualmente a integridade de arquivos essenciais para a operação de todo o sistema e, em especial, do firewall, comparando-os com as somas de verificação de referência. Ela pode detectar alterações não autorizadas e garantir que os scripts do sistema e os arquivos executáveis correspondam ao firmware publicado.

Você pode executar uma verificação por demanda ou programar uma verificação.

Uma verificação por demanda só pode ser executada em um dispositivo CPE.

Para fazer isso, acesse o menu **Modelos de CPE** do orquestrador, selecione um modelo e, no menu SD-WAN, acesse a guia "Verificações de CPE", clique no botão "Executar" na seção "Verificação de integridade" em "Verificação manual".

Uma ferramenta é iniciada no CPE para executar a verificação e enviar as informações para o registro de sistema do CPE.

Ao mesmo tempo, na seção "Verificação de integridade", em "Verificação manual", é indicado que a tarefa foi executada, juntamente com a data e a hora da execução. O status também é exibido aqui.

O orquestrador também exibe o status e o resultado da verificação na interface do usuário do dispositivo CPE, no menu "Principal", na seção "Gerenciamento fora da banda". Após o início, a tarefa "Verificação de integridade" tem o status "Em execução". Em seguida, dependendo do resultado, o CPE envia o status "Sucesso" ou "Erro" ao orquestrador.

Uma verificação programada pode ser configurada em um modelo de CPE ou em um dispositivo CPE.

Para configurar isso, acesse o menu "Modelos de CPE" do orquestrador, selecione um modelo e, em seguida, acesse o menu SD-WAN → guia "Verificações de CPE" e ative o botão de alternância "Verificação de integridade" em "Programação de verificações".

Em um dispositivo CPE, primeiro você precisa ativar o botão de alternância "Substituir".

Agora você pode definir o intervalo entre as verificações.

Uma ferramenta é iniciada no CPE para executar a verificação e enviar as informações para o registro de sistema do CPE.

O orquestrador também exibe o status e o resultado da verificação na interface do usuário do dispositivo CPE, no menu "Principal", na seção "Gerenciamento fora da banda". ????

Além disso, você pode bloquear a transmissão de tráfego em caso de verificações malsucedidas.

Registrar dispositivos CPE

Os seguintes cenários existem para o registro de dispositivos CPE:

- Registrar um dispositivo CPE usando a tecnologia Zero Touch Provisioning (ZTP). Este cenário se aplica a novos dispositivos CPE que não foram registrados anteriormente.
- Implementar um dispositivo vCPE na plataforma de virtualização VMware e registrá-lo usando a tecnologia Zero Touch Provisioning. Este cenário se aplica a dispositivos CPE virtuais implementados em máquinas virtuais.
- Registro repetido de um dispositivo CPE. Este cenário se aplica a dispositivos CPE registrados anteriormente que foram excluídos.

Ao registrar um dispositivo CPE, não é necessário estabelecer conexão com os servidores de atualização e ativação de licenças da Kaspersky nem com os servidores da KSN (Kaspersky Security Network). Se um erro ocorrer durante o registro de um dispositivo CPE, é possível retomar o registro do dispositivo.

Cenário: registro automático de um dispositivo CPE usando a tecnologia Zero Touch Provisioning.

É possível registrar novos dispositivos CPE usando o Zero Touch Provisioning (ZTP). O ZTP permite que um dispositivo CPE estabeleça uma conexão automática ao orquestrador.

Ao usar o ZTP, gere uma URL com as configurações básicas do dispositivo CPE. As *configurações básicas* são aquelas necessárias para conectar automaticamente um dispositivo CPE ao orquestrador. Para concluir o registro, conecte o dispositivo do administrador ao dispositivo CPE e acesse a URL de configurações básicas gerada no dispositivo do administrador.

O cenário de registro ZTP para um dispositivo CPE envolve as seguintes etapas:

1. **Criar um modelo de CPE**

   Crie e configure um modelo de CPE. Para obter detalhes sobre o gerenciamento de modelos de CPE, consulte Gerenciar modelos de CPE. É possível usar o modelo de CPE criado para configurar outros dispositivos CPE.

2. **Adicionar um dispositivo CPE**

   Adicione um dispositivo CPE. Ao adicionar o dispositivo CPE, atribua o modelo de CPE criado a ele e selecione se o dispositivo CPE deve ser ligado automaticamente após o registro. O dispositivo CPE adicionado tem o status **Aguardando**. Para obter detalhes sobre o gerenciamento de dispositivos CPE, consulte Gerenciar dispositivos CPE.

3. **Autenticação de dois fatores (etapa opcional)**

   Para registrar seu dispositivo CPE com segurança, use a autenticação de dois fatores.

4. **Gerar uma URL com configurações básicas**

   Gere uma URL com as configurações básicas do dispositivo CPE.

5. **Registrar o dispositivo CPE**

   Faça o seguinte:

   1. Conecte o dispositivo do administrador à porta LAN do dispositivo CPE.

      O dispositivo do administrador recebe um endereço IP e o endereço IP do gateway padrão via DHCP. O endereço IP do gateway padrão recebido é o endereço IP do dispositivo CPE.

   2. Acesse a URL de configurações básicas do dispositivo CPE gerada no dispositivo do administrador de uma das seguintes formas:

      - Na barra de endereço do navegador, insira a URL de configurações básicas do dispositivo CPE e pressione **Enter**.
      - Abra o arquivo HTML salvo ao gerar a URL de configurações básicas do dispositivo CPE.

   3. Na página aberta, clique no botão **Aplicar configuração**.

   O dispositivo CPE automaticamente se conecta ao orquestrador, se associa ao dispositivo CPE adicionado na interface da Web do orquestrador e se registra. Um dispositivo CPE registrado tem o status **Registrado** e está no estado **Ativado** ou **Desativado**.

6. **Ativar o dispositivo CPE (etapa opcional)**

   Se, ao adicionar o dispositivo CPE, tenha sido especificado que ele não deve ser ativado automaticamente, ative o dispositivo CPE. Um dispositivo CPE ativado tem o status **Registrado** e está no estado **Ativado**.

7. **Ativar a criptografia de tráfego no dispositivo CPE (etapa opcional)**

   Para usar a criptografia de tráfego no dispositivo CPE, ative-a para todo o dispositivo ou para um link específico.

Cenário: implementar um dispositivo vCPE na plataforma de virtualização VMware e registrá-lo usando a tecnologia Zero Touch Provisioning

É possível implementar um dispositivo vCPE na plataforma de virtualização VMware usando um modelo de OVF e, em seguida, registrar o dispositivo usando ZTP.

O *modelo de OVF* é o arquivo comprimido knaas-cpe_<versão do firmware>.release.<número da versão da solução>.combined.adm64-legacy.vKESR-M1-esxi.tar.gz que pode ser encontrado no diretório /cpe do kit de distribuição; o arquivo comprimido inclui os seguintes arquivos:

- vKESR.mf contém o hash SHA256 dos arquivos do modelo de OVF.
- vKESR.nvram contém o estado do BIOS da máquina virtual.

- vKESR.ovf é o descritor que contém informações sobre as configurações da máquina virtual.
- vKESR.vmdk é a imagem do disco da máquina virtual.

É necessário baixar o modelo de OVF e extraí-lo no dispositivo local antes de executar este cenário.

O cenário para a implementação na plataforma de virtualização VMware e o registro ZTP de um dispositivo vCPE envolve as seguintes etapas:

1. **Criar um modelo de vCPE**

   Crie e configure um modelo de vCPE. Para obter detalhes sobre o gerenciamento de modelos de vCPE, consulte Gerenciar modelos de vCPE. É possível usar o modelo de vCPE criado para configurar outros dispositivos vCPE.

2. **Adicionar um dispositivo vCPE**

   Adicione um dispositivo vCPE. Ao adicionar um dispositivo vCPE:

   - Especifique o modelo de vCPE criado.
   - Selecione se deseja que o dispositivo vCPE seja ligado automaticamente após o registro.
   - Especifique um DPID temporário do dispositivo vCPE, por exemplo, `DPID temporário`.

   O dispositivo vCPE adicionado tem o status **Aguardando**. Para obter detalhes sobre o gerenciamento de dispositivos vCPE, consulte Gerenciar dispositivos CPE.

3. **Autenticação de dois fatores (etapa opcional)**

   Para registrar seu dispositivo vCPE com segurança, use a autenticação de dois fatores.

4. **Gerar uma URL com configurações básicas**

   Gere uma URL com as configurações básicas do dispositivo vCPE.

5. **Implementar um dispositivo vCPE na plataforma de virtualização VMware**

   Na interface da Web da plataforma de virtualização VMware, crie uma máquina virtual para implementar o dispositivo vCPE. Certifique-se de que a máquina virtual sendo criada atenda aos requisitos de hardware e software. Ao criar a máquina virtual:

   1. Selecione como deseja criar a máquina virtual, usando o padrão OVF ou um arquivo OVA.
   2. Ao selecionar arquivos VDMK, especifique os arquivos do modelo de OVF extraídos no dispositivo local.
   3. Ao definir as configurações avançadas, especifique a URL gerada com as configurações básicas.

   Para obter detalhes sobre como criar máquinas virtuais, consulte a documentação oficial da VMware.

   Se as configurações forem aplicadas com êxito, o dispositivo vCPE se conecta automaticamente ao orquestrador e é exibido na interface da Web do orquestrador com o status **Desconhecido**.

6. **Registrar um dispositivo vCPE**

   Altere o DPID temporário especificado ao adicionar o dispositivo vCPE ao DPID real do dispositivo vCPE. O DPID real do dispositivo vCPE é o nome do host da máquina virtual na qual o dispositivo está implementado. O nome do host da máquina virtual é exibido na interface da Web da plataforma de virtualização VMware.

   O dispositivo vCPE é vinculado ao dispositivo vCPE adicionado na interface da Web do orquestrador e se registra. Um dispositivo vCPE registrado tem o status **Registrado** e está no estado **Ativado** ou **Desativado**.

7. **Ativar o vCPE (etapa opcional)**

   Se, ao adicionar o dispositivo vCPE, tenha sido especificado que ele não deve ser ativado automaticamente, ative o dispositivo vCPE. Um dispositivo vCPE ativado tem o status **Registrado** e está no estado **Ativado**.

Cenário: registrar novamente um dispositivo CPE

Ao excluir um dispositivo CPE, as configurações básicas são mantidas nele. É possível registrar um CPE remoto novamente sem usar o ZTP.

Ao registrar um dispositivo CPE novamente, não é possível usar a autenticação de dois fatores. Para usar a autenticação de dois fatores, registre o dispositivo CPE usando o ZTP.

O cenário de novo registro do dispositivo CPE envolve as seguintes etapas:

1. **Restaurar o firmware do dispositivo CPE para a condição inicial**

   Conecte-se ao dispositivo CPE por meio de uma conexão SSH. Para isso, especifique o endereço IP e insira as credenciais do dispositivo CPE. Então, execute o seguinte comando:

   ```
   firstboot && reboot
   ```

2. **Criar um modelo de CPE**

   Crie e configure um modelo de CPE. Para obter detalhes sobre o gerenciamento de modelos de CPE, consulte Gerenciar modelos de CPE. É possível usar o modelo de CPE criado para configurar outros dispositivos CPE.

3. **Conectar o dispositivo CPE ao orquestrador**

   Desconecte e reconecte o cabo de alimentação do dispositivo CPE para que ele seja redefinido e conectado ao orquestrador. Se a conexão for bem-sucedida, o dispositivo CPE será exibido na interface da Web do orquestrador com o status **Desconhecido**.

4. **Registrar um dispositivo CPE manualmente**

   Registre o dispositivo CPE manualmente. Ao registrar o dispositivo CPE manualmente, atribua o modelo de CPE criado a ele e selecione se o dispositivo CPE deve ser ligado automaticamente após o registro. Um dispositivo registrado tem o status **Registrado** e está no estado **Ativado** ou **Desativado**. Para obter detalhes sobre o gerenciamento de dispositivos CPE, consulte Gerenciar dispositivos CPE.

5. **Ativar o dispositivo CPE (etapa opcional)**

   Se, ao registrar manualmente o dispositivo CPE, tenha sido especificado que ele não deve ser ligado automaticamente, ative o dispositivo CPE. Um dispositivo CPE ativado tem o status **Registrado** e está no estado **Ativado**.

Retomar o registro do dispositivo CPE em caso de erro

Se um erro ocorrer ao registrar um dispositivo CPE, o status do dispositivo é alterado para **Suspensa** e o registro não é concluído.

Para retomar o registro de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Na coluna **Status**, clique no status do dispositivo CPE.

   O log da solicitação de serviço é exibido.

3. Clique na etapa em que o erro ocorreu para ver informações sobre as possíveis causas, bem como os passos para a correção do erro.

4. Para cancelar o registro do dispositivo CPE, clique em **Cancelar**.

5. Após concluir os passos para a correção do erro, clique em **Retomar** para retomar o registro do dispositivo CPE. Em alguns casos, o dispositivo CPE precisa ser reiniciado após a retomada do processo de registro.

O dispositivo CPE é registrado novamente.

Caso não consiga registrar um dispositivo CPE, recomendamos entrar em contato com o Suporte Técnico da Kaspersky.

Gerenciar modelos de CPE

É possível visualizar a tabela de modelos de CPE na seção **SD-WAN →Modelos de CPE**. As informações sobre modelos de CPE são exibidas nas seguintes colunas da tabela:

- **ID** é o ID do modelo de CPE.
- **Nome** é o nome do modelo de CPE.
- **Utilização** especifica se os dispositivos CPE usam um modelo de CPE:
  - **Sim**.
  - **Não**.
- **Atualizado** é a data e hora em que as configurações do modelo de CPE foram modificadas pela última vez.
- **Usuário** é o nome do usuário que criou o modelo de CPE.
- **Proprietário** é o locatário ao qual o modelo de CPE pertence.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

É possível gerenciar as configurações de modelos de CPE nas seguintes guias:

- **Informações** são as informações básicas sobre o modelo de CPE. É possível editar o nome do modelo de CPE no campo **Nome**.
- **Múltiplos caminhos** são as configurações de caminho.

- **Desativação** são configurações para remover e desativar automaticamente o dispositivo CPE.
- **Criptografia** são as configurações de criptografia de tráfego.
- **Scripts** são scripts para configuração adicional do dispositivo CPE.
- **SD-WAN** são configurações de conexão de um dispositivo CPE à rede SD-WAN. As seguintes guias são exibidas nesta guia:
  - **Configurações gerais** contém as configurações de conexão de um dispositivo CPE com orquestrador e controlador.
  - **Interfaces** contém interfaces SD-WAN.
- **Topologia** contém tags de topologia para estabelecer links entre dispositivos CPE.
- **Rede** contém interfaces de rede.
- **BGP** contém as configurações do protocolo BGP para trocar rotas entre dispositivos CPE e dispositivos de rede externos.
- **VRF** contém tabelas de roteamento e encaminhamento virtual.
- **OSPF** abrange o protocolo OSPF para troca de rotas entre dispositivos CPE e dispositivos de rede externos. As seguintes guias são exibidas nesta guia:
  - **Configurações gerais** contém configurações básicas do protocolo OSPF.
  - **Áreas OSPF** contém áreas OSPF.
  - **Interfaces OSPF** contém interfaces OSPF.
- **Filtros de roteamento** contém configurações para filtrar rotas e pacotes de tráfego entre dispositivos CPE e dispositivos de rede externos. As seguintes guias são exibidas nesta guia:
  - **Listas de controle de acesso** contém listas de controle de acesso (ACLs).
  - **Listas de prefixos** contém listas de prefixos.
  - **Mapas de roteamento** contém mapas de roteamento.
- **BFD** abrange o protocolo BFD para a detecção de falhas de roteamento entre dispositivos CPE e dispositivos de rede externos.
- **Rotas estáticas** contém rotas estáticas.
- **Multicast** contém configurações para transmissão de tráfego multicast entre dispositivos CPE e dispositivos de rede externos usando os protocolos PIM e IGMP. As seguintes guias são exibidas nesta guia:
  - **Configurações gerais** contém configurações básicas de PIM.
  - **Interfaces** contém interfaces multicast.

- **VRRP** abrange o protocolo VRRP para alta disponibilidade de dispositivos CPE. As seguintes guias são exibidas nesta guia:
  - **Instâncias VRRP** contém instâncias VRRP.
  - **Grupos de instâncias VRRP** contém grupos de instâncias VRRP.
- **CFM** contém configurações da funcionalidade de Gerenciamento de falhas de conectividade (CFM).
- **Monitoramento** contém as configurações de monitoramento do dispositivo CPE.
- **Serviços de transporte** contém os serviços de transporte.
- **Registro** contém as configurações de registro.
- **NTP** contém os servidores NTP para sincronização de tempo.
- **VIM** contém as configurações de VIM. Essa guia só é exibida se o tipo **uCPE** for selecionado ao criar o modelo.

Criar um modelo de CPE

Para criar um modelo de CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.
   Uma tabela de modelos de CPE é exibida.
2. Na parte superior da página, clique em **+ Modelo de CPE**.
3. Na janela aberta, no campo **Nome**, insira o nome do modelo de CPE.
4. Na lista suspensa **Tipo**, selecione o tipo de modelo de CPE:
   - **CPE** para um modelo de dispositivo CPE padrão. Essa é a configuração padrão.
   - **uCPE** para um modelo de dispositivo uCPE. Os dispositivos uCPE incluem um hipervisor, que permite implementar funções de rede virtual e VIMs no dispositivo uCPE.
5. Clique em **Criar**.

   O modelo de CPE é criado e exibido na tabela.

É necessário configurar o modelo de CPE criado. Para obter detalhes sobre o gerenciamento de modelos de CPE, consulte Gerenciar modelos de CPE.

Importar um modelo de CPE

É possível exportar um modelo de CPE e depois importá-lo para outro modelo de CPE. As configurações do modelo de CPE são especificadas de acordo com as configurações do modelo de CPE importado. Durante a importação, selecione as guias que deseja deixar inalteradas.

Para importar um modelo de CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE que deseja exportar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Na parte superior da área de configurações, em **Ações**, clique em **Exportar**.

   Um arquivo comprimido TAR.GZ com os seguintes dados é salvo no dispositivo local:

   - Um arquivo com a descrição do modelo de CPE no formato XML. A versão do modelo é indicada na descrição.
   - Arquivos de script.
   - Arquivos necessários para executar scripts, como certificados SSL.

   O arquivo não contém informações sobre dispositivos CPE que usam o modelo de CPE.

4. Clique no modelo de CPE para o qual deseja importar outro modelo de CPE.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

5. Na parte superior da área de configurações, em **Ações**, clique em **Importar**.

6. Na janela aberta, desmarque as caixas de seleção ao lado das guias do modelo de CPE que deseja manter inalteradas após a importação.

7. No campo **Arquivo**, especifique o caminho para o arquivo TAR.GZ.

8. Clique em **Importar**.

As configurações do modelo de CPE são alteradas de acordo com as configurações do modelo de CPE importado.

Clonar um modelo de CPE

É possível clonar um modelo de CPE para criar um modelo idêntico com um nome diferente.

Para clonar um modelo de CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE que deseja clonar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Na parte superior da área de configurações, em **Ações**, clique em **Clonar**.

4. Na janela aberta, insira o nome do novo modelo de CPE.

5. Clique em **Clonar**.

Um clone do modelo de CPE com o novo nome é criado e exibido na tabela.

Exportar configurações de conexão do orquestrador e do controlador e interfaces SD-WAN de um modelo de CPE

Para exportar configurações de conexão do orquestrador e do controlador e interfaces SD-WAN de um modelo de CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE do qual deseja exportar as configurações de conexão do orquestrador e do controlador e as interfaces SD-WAN.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Na parte superior da área de configurações, em **Ações**, clique em **Exportar configurações de SD-WAN**.

Um arquivo JSON denominado <Nome do modelo>sdwan-config é salvo no dispositivo local.

Exportar interfaces de rede de um modelo de CPE

Para exportar interfaces de rede de um modelo de CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE do qual deseja exportar interfaces de rede.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Na parte superior da área de configurações, em **Ações**, clique em **Exportar interfaces de rede**.

Um arquivo no formato JSON com o nome <Nome do modelo>-network-config é salvo no dispositivo local.

Visualizar o uso de um modelo de CPE

Se necessário, é possível verificar quais dispositivos CPE estão usando o modelo de CPE. Por exemplo, se um modelo de CPE estiver em uso, ele não pode ser excluído.

Para ver se um modelo de CPE está sendo usado:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE cujas informações de uso deseja visualizar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Na parte superior da área de configurações, em **Ações**, clique em **Mostrar CPEs associados**.

A seção **CPE** é exibida com uma tabela de dispositivos CPE que estão usando o modelo de CPE.

Excluir um modelo de CPE

Não é possível excluir um modelo de CPE se ele estiver sendo usado por pelo menos um dispositivo CPE. Para excluir um modelo de CPE que está sendo usado por dispositivos CPE, primeiro exclua os dispositivos CPE. É possível verificar quais dispositivos CPE estão usando o modelo de CPE.

Os modelos de CPE excluídos não podem ser restaurados.

Para excluir um modelo de CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE que deseja excluir.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

O modelo de CPE é excluído e não é mais exibido na tabela.

Gerenciar dispositivos CPE

É possível visualizar a tabela de dispositivos CPE na seção **SD-WAN** → **CPE**.

Use filtros na parte superior da tabela para filtrá-la rapidamente por status do dispositivo, status da conexão, status de energia e período.

As informações sobre dispositivos CPE são exibidas nas seguintes colunas da tabela:

- **DPID** é o DPID do dispositivo CPE.
- **S/N** é o número de série do dispositivo CPE.
- **Modelo** é o modelo do dispositivo CPE.
- **Tipo de switch** é o tipo de switch de software em que o firmware do dispositivo CPE é baseado (OVS ou SWOS).
- **Versão do SW** é a versão do firmware do dispositivo CPE. Firmwares desatualizados são destacados em laranja.
- **Nome** é o nome do dispositivo CPE.
- **Função** é a função do dispositivo CPE:
  - **CPE**
  - **Gateway**
- **Status** é o status do dispositivo CPE.
  - **Desconhecido** significa que o dispositivo CPE está conectado ao orquestrador, mas não está registrado.
  - **Aguardando** significa que o dispositivo CPE foi adicionado à interface da Web do orquestrador, mas não está conectado ao orquestrador.
  - **Registrando** significa que o dispositivo CPE está sendo registrado.
  - **Erro** significa que ocorreu um erro ao registrar o dispositivo CPE.
  - **Registrado** significa que o dispositivo CPE foi registrado.
  - **Configuração**significa que scripts estão sendo iniciados no dispositivo CPE.
  - **Suspensa** significa que ocorreu um erro ao registrar o dispositivo CPE e o registro não foi concluído.

- **Estado** é o estado do dispositivo CPE:
  - **Ativado** significa que o modelo de CPE atribuído foi aplicado ao dispositivo CPE no lado do orquestrador. No lado do controlador, o dispositivo CPE pode ser usado para retransmitir tráfego.
  - **Desativado** (no status **Aguardando**) significa que o modelo de CPE atribuído não foi aplicado ao dispositivo CPE no lado do orquestrador. No lado do controlador, o dispositivo CPE não pode ser usado para retransmitir tráfego.
  - **Desativado** (no status **Registrado**) significa que o orquestrador não responde às solicitações da API REST do dispositivo CPE. No lado do controlador, a transmissão do tráfego por meio de links é bloqueada para o dispositivo CPE.
- **Conexão** contém informações sobre se o dispositivo CPE está conectado ao controlador:
  - **Conectado**
  - **Desconectado**
- **Tags de topologia** contém tags de topologia que foram atribuídas ao dispositivo CPE.
- **Fragmentação** é o resultado da verificação da fragmentação de pacotes de tráfego no dispositivo CPE:
  - **Sem suporte** significa que o dispositivo CPE não pode transmitir pacotes fragmentados.
  - **Desconhecido** significa que a fragmentação de pacotes não pode ser verificada no dispositivo CPE.
  - **Com suporte** significa que o dispositivo pode transmitir pacotes fragmentados.
- **Locatário de transporte** é o locatário de transporte ao qual o dispositivo CPE é adicionado. O dispositivo CPE faz conexão com o controlador da instância SD-WAN implementada para o locatário de transporte.
- **Locatário do cliente** é o locatário cliente ao qual o dispositivo CPE é adicionado. O locatário cliente pode gerenciar o dispositivo CPE no portal de autoatendimento.
- **Modelo de CPE** é o modelo de CPE usado pelo dispositivo CPE.
- **Localização** é o endereço de localização do dispositivo CPE.
- **IP de gerenciamento** é o endereço IP atribuído ao dispositivo CPE pela sub-rede de gerenciamento.
- **Controladores** são os endereços IP e o número da porta dos nós do controlador aos quais o dispositivo CPE está conectado.
- **Gateways** são os endereços IP e os números de porta dos gateways aos quais o dispositivo CPE está conectado.
- **Rede móvel** é a rede móvel à qual o dispositivo CPE está conectado.
- **Registrado** é a data e hora em que o dispositivo CPE foi registrado.
- **Atualização** é a data e hora em que as configurações do dispositivo CPE foram modificadas pela última vez.
- **Usuário** é o nome do usuário que criou o dispositivo CPE.

- **Status de energia** é o status de energia do dispositivo CPE:
  - **OK**
  - **Falha da PSU**
  - **Bateria**
  - **Desconhecido**

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

É possível visualizar e gerenciar as configurações do dispositivo CPE clicando no nome dele na tabela para abrir uma janela e selecionar uma seção da barra lateral:

- **Configuração** são as informações básicas sobre o dispositivo CPE. É possível visualizar as informações nas seguintes colunas da tabela **Informações do dispositivo**:
  - **Modelo** é o modelo do dispositivo CPE.
  - **Versão do SW** é a versão do firmware do dispositivo CPE. Firmwares desatualizados são destacados em laranja.
  - **Controlador** são os endereços IP e o número da porta dos nós do controlador aos quais o dispositivo CPE está conectado.
  - **Gateways** são os endereços IP e os números de porta dos gateways aos quais o dispositivo CPE está conectado.
  - **Usuário** é o nome do usuário que criou o dispositivo CPE.
  - **Registrado** é a data e hora em que o dispositivo CPE foi registrado.
  - **Atualização** é a data e hora em que as configurações do dispositivo CPE foram modificadas pela última vez.
  - **IP de gerenciamento** é o endereço IP atribuído ao dispositivo CPE pela sub-rede de gerenciamento.
  - **Estado** é o estado do dispositivo CPE:
    - **Ativado** significa que o modelo de CPE atribuído foi aplicado ao dispositivo CPE no lado do orquestrador. No lado do controlador, o dispositivo CPE pode ser usado para retransmitir tráfego.
    - **Desativado** (no status **Aguardando**) significa que o modelo de CPE atribuído não foi aplicado ao dispositivo CPE no lado do orquestrador. No lado do controlador, o dispositivo CPE não pode ser usado para retransmitir tráfego.
    - **Desativado** (no status **Registrado**) significa que o orquestrador não responde às solicitações da API REST do dispositivo CPE. No lado do controlador, a transmissão do tráfego por meio de links é bloqueada para o dispositivo CPE.
  - **Conexão** contém informações sobre se o dispositivo CPE está conectado ao controlador:
    - **Conectado**
    - **Desconectado**

É possível inserir uma breve descrição do dispositivo CPE no campo **Descrição** e visualizar as tarefas sendo executadas pelo orquestrador na tabela **Gerenciamento fora da banda**.

- **Monitoramento** são os resultados de monitoramento do dispositivo CPE.
- **Problemas** são problemas que ocorreram enquanto o dispositivo CPE estava operacional. Em caso de problemas, um ponto de exclamação vermelho é exibido ao lado da guia.
- **Criptografia** são as configurações de criptografia de tráfego.
- **Solicitações de serviço** são solicitações de serviço do dispositivo CPE.
- **Tags** são tags para agrupar dispositivos CPE.
- **Scripts** são scripts para configuração adicional do dispositivo CPE.
- **SD-WAN** são configurações de conexão de um dispositivo CPE à rede SD-WAN. As seguintes guias são exibidas nesta guia:
  - **Configurações gerais** contém as configurações de conexão de um dispositivo CPE com orquestrador e controlador.
  - **Interfaces** contém interfaces SD-WAN.
- **Topologia** contém tags de topologia para estabelecer links entre dispositivos CPE.
- **Rede** contém interfaces de rede.
- **DHCP** contém configurações de DHCP.
- **Firewall** contém configurações de firewall.
- **VRF** contém tabelas de roteamento e encaminhamento virtual.
  - **BGP** contém as configurações do protocolo BGP para trocar rotas entre dispositivos CPE e dispositivos de rede externos.
- **OSPF** abrange o protocolo OSPF para troca de rotas entre dispositivos CPE e dispositivos de rede externos. As seguintes guias são exibidas nesta guia:
  - **Configurações gerais** contém configurações básicas do protocolo OSPF.
  - **Áreas OSPF** contém áreas OSPF.
  - **Interfaces OSPF** contém interfaces OSPF.
- **Filtros de roteamento** contém configurações para filtrar rotas e pacotes de tráfego entre dispositivos CPE e dispositivos de rede externos. As seguintes guias são exibidas nesta guia:
  - **Listas de controle de acesso** contém listas de controle de acesso (ACLs).
  - **Listas de prefixos** contém listas de prefixos.
  - **Mapas de roteamento** contém mapas de roteamento.
- **PBR** contém configurações de roteamento baseado em política (PBR).

- **BFD** abrange o protocolo BFD para a deteção de falhas de roteamento entre dispositivos CPE e dispositivos de rede externos.
- **Rotas estáticas** contém rotas estáticas.
- **Multicast** contém configurações para transmissão de tráfego multicast entre dispositivos CPE e dispositivos de rede externos usando os protocolos PIM e IGMP. As seguintes guias são exibidas nesta guia:
  - **Configurações gerais** contém configurações básicas de PIM.
  - **Interfaces** contém interfaces multicast.
- **VRRP** abrange o protocolo VRRP para alta disponibilidade de dispositivos CPE. As seguintes guias são exibidas nesta guia:
  - **Instâncias VRRP** contém instâncias VRRP.
  - **Grupos de instâncias VRRP** contém grupos de instâncias VRRP.
- **CFM** contém configurações da funcionalidade de Gerenciamento de falhas de conectividade (CFM).
- **UNIs** são UNIs no dispositivo CPE.
- **Modems** são configurações do modem do dispositivo CPE.
- **Links** contém configurações de link.
- **Múltiplos caminhos** são as configurações de caminho.
- **Ativação** são configurações de autenticação de dois fatores do dispositivo CPE.
- **Desativação** são configurações para remover e desativar automaticamente o dispositivo CPE.
- **Registro** contém as configurações de registro.
- **NetFlow**contém configurações básicas do NetFlow.
- **NTP** exibe os servidores NTP usados para a sincronização de tempo.
- **Informações de diagnóstico** exibe solicitações de informações de diagnóstico do dispositivo CPE.
- **Utilitários** exibe utilitários para diagnosticar dispositivos CPE.

Adicionar dispositivos CPE

É necessário adicionar um dispositivo CPE caso esteja registrando-o automaticamente (ZTP). Ao adicionar um dispositivo CPE, especifique o DPID que será usado para fazer a correspondência do registro adicionado ao dispositivo CPE que será conectado mais tarde. É possível adicionar um dispositivo CPE para a instância SD-WAN atual, um locatário ou uma instância SD-WAN diferente. É possível adicionar um dispositivo individual ou dispositivos de importação em massa com configurações de um arquivo CSV.

Para adicionar um dispositivo CPE:

1. Adicione um dispositivo CPE de uma das seguintes formas:

   - Se você quiser adicionar um dispositivo CPE para a instância SD-WAN atual, no menu, vá para a seção **SD-WAN → CPE** e, na parte superior da página, clique em **+ Adicionar**.

   - Se você quiser adicionar um dispositivo CPE para uma locação, vá para a seção **Locatários**, clique na locação criada e, na guia **CPEs**, clique no botão **+ Adicionar**.

   - Se você quiser adicionar um dispositivo CPE para uma instância SD-WAN diferente, vá para a subseção **SD-WAN → Instâncias SD-WAN**, clique em uma instância SD-WAN implementada e, na parte superior da área de configurações, em **Ações**, clique em **Adicionar CPE**.

2. Na janela aberta, no campo **Nome**, insira o nome do dispositivo CPE.

3. No campo **DPID**, insira o DPID do dispositivo CPE. O DPID pode ser encontrado na caixa do dispositivo CPE.

   Se o dispositivo CPE não tiver um DPID, especifique um DPID temporário, por exemplo, `DPID temporário`. É possível substituir o DPID temporário pelo DPID real.

4. Na lista suspensa **Estado**, selecione o estado do dispositivo CPE após o registro:

   - **Ativado** para aplicar um modelo de CPE ao dispositivo CPE e usá-lo para retransmitir o tráfego. Essa é a configuração padrão.

   - **Desativado** para não aplicar um modelo de CPE ao dispositivo CPE.

5. Se necessário, no campo **Descrição**, insira uma breve descrição do dispositivo CPE.

6. Caso esteja adicionando um dispositivo CPE a uma instância SD-WAN, na lista suspensa **Locatário**, selecione o locatário de transporte ao qual deseja adicionar o dispositivo CPE. O dispositivo CPE faz conexão com o controlador da instância SD-WAN implementada para o locatário de transporte. É possível selecionar um pool de instâncias SD-WAN.

7. Na lista suspensa **Locatário do cliente**, selecione o locatário cliente ao qual deseja adicionar o dispositivo CPE. O locatário cliente pode gerenciar o dispositivo CPE no portal de autoatendimento.

8. Para criar uma UNI no dispositivo CPE usando um modelo de UNI, na lista suspensa **Modelo de UNI**, selecione o modelo de UNI criado.

9. Na lista suspensa **Modelo de CPE**, selecione o modelo de CPE criado que deseja usar para configurar o dispositivo CPE.

10. Na lista suspensa **Modelo NetFlow**, selecione o modelo de NetFlow criado que deseja usar para definir as configurações básicas de NetFlow no dispositivo CPE.

11. Na lista suspensa **Modelo de firewall**, selecione o modelo de firewall criado que deseja usar para configurar o firewall do dispositivo CPE.

12. Clique em **Next** e especifique o endereço do local do dispositivo CPE no campo **Endereço**. Ao inserir o endereço, é solicitado que você selecione um endereço em uma lista suspensa.

    O endereço é exibido no mapa.

13. Clique em **Concluído**.

O dispositivo é adicionado, seu status muda para **Aguardando**, e você obtém um dos seguintes resultados:

- Caso tenha adicionado o dispositivo CPE para a instância SD-WAN atual, o dispositivo CPE é exibido na tabela.
- Se você adicionou um dispositivo CPE para uma locação, esse dispositivo CPE aparecerá na área de configurações do locatário na guia **CPEs**.
- Caso tenha adicionado um dispositivo CPE a uma instância SD-WAN diferente, o portal de autoatendimento é aberto em uma nova guia do navegador. Você é automaticamente conectado ao portal de autoatendimento e direcionado para a subseção **CPE**. O dispositivo CPE é adicionado à tabela.

Importação em massa de dispositivos CPE de um arquivo CSV

Caso precise adicionar muitos dispositivos CPE ao mesmo tempo, é possível usar o recurso de importação em massa. Antes de importar dispositivos CPE, especifique as configurações deles em um arquivo CSV. O arquivo CSV para a importação deve atender aos seguintes requisitos:

- A primeira linha no arquivo CSV contém os cabeçalhos.
- A ordem dos cabeçalhos não é importante.
- O arquivo importado deve ter a extensão `csv`.
- O tamanho máximo do arquivo é 10.485.760 bytes.
- O número máximo de linhas no arquivo é 25.001 (25.000 linhas de dados + 1 linha de cabeçalho).

Se estiver importando em um locatário, os locatários cliente e de transporte serão especificados automaticamente pelo orquestrador e os valores correspondentes do arquivo CSV serão ignorados.

Para obter uma descrição detalhada das colunas no arquivo, consulte a tabela neste artigo. Você também pode baixar um arquivo de exemplo na janela de importação.

Para importar dispositivos CPE de um arquivo:

1. Prepare o arquivo CSV para importação.
2. No menu, acesse a seção **SD-WAN** → **CPE**; na parte superior da página, clique no ícone ⌄ na parte direita do **+ CPE** para abrir a lista suspensa e selecione **Importação em massa de CSV**.
3. Na janela aberta, selecione o arquivo CSV preparado e carregue-o no orquestrador.

   Depois que o arquivo CSV é carregado, o orquestrador valida as linhas no arquivo.

4. Quaisquer erros encontrados são listados na janela de importação. A lista de erros é dividida em guias, dependendo do tipo de erro:

   - **Formato de linha inválido**
   - **Sem monitoramento**
   - **Objeto não encontrado**
   - **Erros de validação**

   Se houver erros de importação, corrija-os no arquivo e tente novamente.

5. Se o arquivo for aprovado na validação sem erros, a importação será iniciada. Durante toda a validação e importação, o dispositivo CPE fica bloqueado (o tempo máximo de bloqueio é de 30 segundos).

Após a importação bem-sucedida, uma mensagem correspondente é exibida, indicando o número de dispositivos adicionados. Os dispositivos são adicionados e exibidos na tabela; o status deles muda para **Aguardando**.

Descrição das colunas do arquivo CSV para a importação em massa de dispositivos CPE

Nome da coluna	Conteúdo da coluna	Processo de validação	Necessário
`Nome`	Nome do dispositivo CPE. String de texto arbitrária.	O mesmo que para adicionar um dispositivo CPE individual.	Necessário
`MACAddress`	6 grupos de 2 números hexadecimais, que podem ser separados por hifens, dois pontos ou nada. Exemplos: • `DE-AD-BE-EF-11-22` • `DE:AD:BE:EF:11:22` • `DEADBEEF1122`	O valor resultante é convertido para o formato DPID: • 8000 é adicionado ao início da linha • Separadores, se houver, são removidos • As letras `a–f` são convertidas em maiúsculas se estiverem em minúsculas. A validação do DPID obtido é a mesma que para adicionar um dispositivo CPE individual.	Necessário
`Estado`	String. Valores possíveis: • `enabled` • `disabled`	O mesmo que para adicionar um dispositivo CPE individual.	Necessário
`Transport Tenant`	Nome do locatário de transporte.	Esse valor é usado para pesquisar o locatário de transporte.	Necessário
`CPE Template`	Nome do modelo de CPE.	Esse valor é usado para pesquisar o modelo de CPE com um proprietário que corresponda ao locatário do qual o CSV está sendo importado.	Necessário
`Modelo de NetFlow`	Nome do modelo de NetFlow.	Esse valor é usado para pesquisar o modelo de NetFlow com um proprietário que corresponda ao locatário do qual o CSV está sendo importado.	Necessário
`Modelo de firewall`	Nome do modelo de firewall.	Esse valor é usado para pesquisar o modelo de firewall com um proprietário que corresponda ao locatário do qual o CSV está sendo importado.	Necessário
`Descrição`	Descrição do dispositivo CPE. String de texto arbitrária.	O mesmo que para adicionar um dispositivo CPE individual.	Opcional
`Customer Tenant`	Nome do locatário do cliente.	Esse valor é usado para pesquisar o locatário do cliente.	Opcional
`Modelo de UNI`	Nome do modelo de UNI.	Esse valor é usado para pesquisar o modelo de UNI com um proprietário que corresponda ao locatário do qual o CSV está sendo importado.	Opcional

Gerar uma URL com configurações básicas do dispositivo CPE

Para o registro automático de um dispositivo CPE, é necessário gerar um endereço da Web com as configurações básicas do dispositivo CPE. Especifique o modelo da URL gerada ao configurar a conexão do dispositivo CPE com orquestrador e controlador. A URL gerada contém as seguintes informações:

- Servidores NTP
- Interfaces de rede
- Configurações para a conexão do dispositivo CPE com orquestrador e controlador e às interfaces SD-WAN
- Certificados
- Configurações de BGP
- O token, caso a autenticação de dois fatores estiver sendo usada
- Tabelas de roteamento e encaminhamento virtual
- Diretórios APN

O tamanho máximo de uma URL com configurações básicas do dispositivo CPE não pode exceder 64 KB.

Para gerar uma URL com as configurações básicas do dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE para o qual deseja gerar uma URL com configurações básicas.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Obter URL de configuração**.

4. Isso abre uma janela; nessa janela, na lista suspensa **Versão**, especifique a versão do firmware do dispositivo CPE para o qual você deseja gerar um endereço da Web com configurações básicas:

   - **Atual**
   - **23,07**

5. Salve a URL com configurações básicas do dispositivo CPE de uma das seguintes formas:

   - Para copiar a URL, clique em **Copiar** ao lado dela.
   - Para salvar o endereço da Web como um arquivo HTML, clique em **Salvar** ao lado dele.

   É necessário conectar um dispositivo do administrador à porta LAN do dispositivo CPE e usar a URL salva com configurações básicas para registrar automaticamente o dispositivo CPE.

Para instalar certificados em um dispositivo CPE com firmware versão 23.07, siga as etapas descritas no artigo Cenário: instalar certificados em um dispositivo CPE com firmware versão 23.07.

Registrar um dispositivo CPE manualmente

É necessário registrar o dispositivo CPE na interface da Web de forma manual ao registrá-lo novamente. O registro não requer conexão com os serviços em nuvem da Kaspersky.

Para registrar um dispositivo CPE manualmente:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE que deseja registrar manualmente.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Registrar**.

4. Na janela aberta, na lista suspensa **Estado**, selecione o estado do dispositivo CPE após o registro:

   - **Ativado** para aplicar um modelo de CPE ao dispositivo CPE e usá-lo para retransmitir o tráfego. Essa é a configuração padrão.
   - **Desativado** para não aplicar um modelo de CPE ao dispositivo CPE.

5. Se necessário, no campo **Descrição**, insira uma breve descrição do dispositivo CPE.

6. Na lista suspensa **Locatário**, selecione o locatário de transporte ao qual deseja adicionar o dispositivo CPE. O dispositivo CPE faz conexão com o controlador da instância SD-WAN implementada para o locatário de transporte. É possível selecionar um pool de instâncias SD-WAN.

7. Na lista suspensa **Locatário do cliente**, selecione o locatário cliente ao qual deseja adicionar o dispositivo CPE. O locatário cliente pode gerenciar o dispositivo CPE no portal de autoatendimento.

8. Para criar uma UNI no dispositivo CPE usando um modelo de UNI, na lista suspensa **Modelo de UNI**, selecione o modelo de UNI criado.

9. Na lista suspensa **Modelo de CPE**, selecione o modelo de CPE criado que deseja usar para configurar o dispositivo CPE.

10. Na lista suspensa **Modelo NetFlow**, selecione o modelo de NetFlow criado que deseja usar para definir as configurações básicas de NetFlow no dispositivo CPE.

11. Na lista suspensa **Modelo de firewall**, selecione o modelo de firewall criado que deseja usar para configurar o firewall do dispositivo CPE.

12. Clique em **Next** e especifique o endereço do local do dispositivo CPE no campo **Endereço**. Ao inserir o endereço, é solicitado que você selecione um endereço em uma lista suspensa.

    O endereço é exibido no mapa.

13. Clique em **Registrar**.

O status do dispositivo CPE muda primeiro para **Registrando** e então para **Registrado**.

Cancelar o registro de um dispositivo CPE

Para cancelar o registro de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE cujo registro deseja cancelar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Anular registro**.

4. Na janela de confirmação, clique em **Anular registro**.

O registro do dispositivo CPE é cancelado e o status do dispositivo muda para **Aguardando**.

Especificar o endereço de um dispositivo CPE

Para especificar o endereço de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE cujo endereço deseja especificar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Definir localização**.

4. Na janela aberta, insira o endereço da localização do dispositivo CPE. Ao inserir o endereço, é solicitado que você selecione um endereço em uma lista suspensa.

   O endereço é exibido no mapa.

5. Clique em **Salvar**.

O endereço do dispositivo CPE é especificado.

Ativar e desativar um dispositivo CPE

Quando um dispositivo CPE é ativado, um modelo de CPE é aplicado a ele. Os dispositivos CPE desativados não podem ser usados para retransmitir o tráfego.

Para ativar ou desativar um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE que deseja ativar ou desativar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Ativar** ou **Desativar**.

O dispositivo CPE é ativado ou desativado.

Reiniciar um dispositivo CPE

Para reiniciar um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE que deseja reiniciar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Reinicialização**.

4. Na janela de confirmação, clique em **Reinicialização**.

O dispositivo CPE é reiniciado.

Desligar um dispositivo CPE

É possível desligar o dispositivo CPE na interface da Web do orquestrador ou desconectando o cabo de alimentação do dispositivo. Quando a energia é desligada na interface da Web do orquestrador, o comando de `desligamento` é enviado ao sistema operacional do dispositivo CPE.

Para desligar o dispositivo CPE na interface da Web do orquestrador:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE que deseja desligar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Desligar**.

4. Na janela de confirmação, clique em **Desligar**.

O dispositivo CPE é desligado.

Conectar-se ao console do dispositivo CPE

Para se conectar ao console de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE a cujo console deseja se conectar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Abrir console SSH**.

Isso abre a janela do console do dispositivo CPE em uma nova guia do navegador.

Visualizar a senha de um dispositivo CPE

Para visualizar a senha de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE cuja senha deseja visualizar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Mostrar senha**.

Isso abre uma janela com a senha do dispositivo CPE.

Exportar configurações de conexão do orquestrador e do controlador e interfaces SD-WAN de um dispositivo CPE

Para exportar configurações de conexão do orquestrador e do controlador e interfaces SD-WAN de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE do qual deseja exportar as configurações de conexão do orquestrador e do controlador e as interfaces SD-WAN.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Exportar configurações de SD-WAN**.

Um arquivo JSON denominado <Nome do modelo>sdwan-config é salvo no dispositivo local.

Exportar interfaces de rede de um dispositivo CPE

Para exportar interfaces de rede de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE do qual deseja exportar interfaces de rede.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior, em **Ações**, clique em **Exportar interfaces de rede**.

Um arquivo no formato JSON com o nome <Nome do modelo>-network-config é salvo no dispositivo local.

Alterar o DPID de um dispositivo CPE

Pode ser necessário editar o DPID nos seguintes cenários:

- Implementar um dispositivo vCPE na plataforma de virtualização VMware com registro automático
- Substituir um dispositivo CPE registrado existente por um novo dispositivo CPE mantendo a antiga configuração de rede (por exemplo, se um dispositivo se tornar inoperável).

Para alterar o DPID de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE cujo DPID deseja alterar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, em **Ações**, clique em **Alterar DPID**.

4. Na janela aberta, insira o novo DPID do dispositivo CPE.

5. Clique em **Salvar**.

O DPID do dispositivo CPE é alterado.

Editar as configurações do dispositivo CPE

Se necessário, é possível editar as configurações do dispositivo CPE. As configurações modificadas podem ser aplicadas imediatamente ou após um atraso usando o agendador de tarefas.

Para editar as configurações do dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE cujas configurações deseja editar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Após selecionar as guias com as configurações do dispositivo CPE que deseja editar, comece a editar as configurações.

4. Selecione uma das opções para salvar as configurações:

   - Caso deseje que as alterações sejam aplicadas instantaneamente, clique no botão **Salvar**.

     As configurações do dispositivo CPE são salvas.

   - Para agendar a aplicação das configurações em um horário específico:

     1. Usando o ícone ⌄ na parte direita do botão **Salvar**, abra o menu de modo de salvamento e selecione **Programação salva**.

        Isso abre a barra lateral para a criação de uma tarefa.

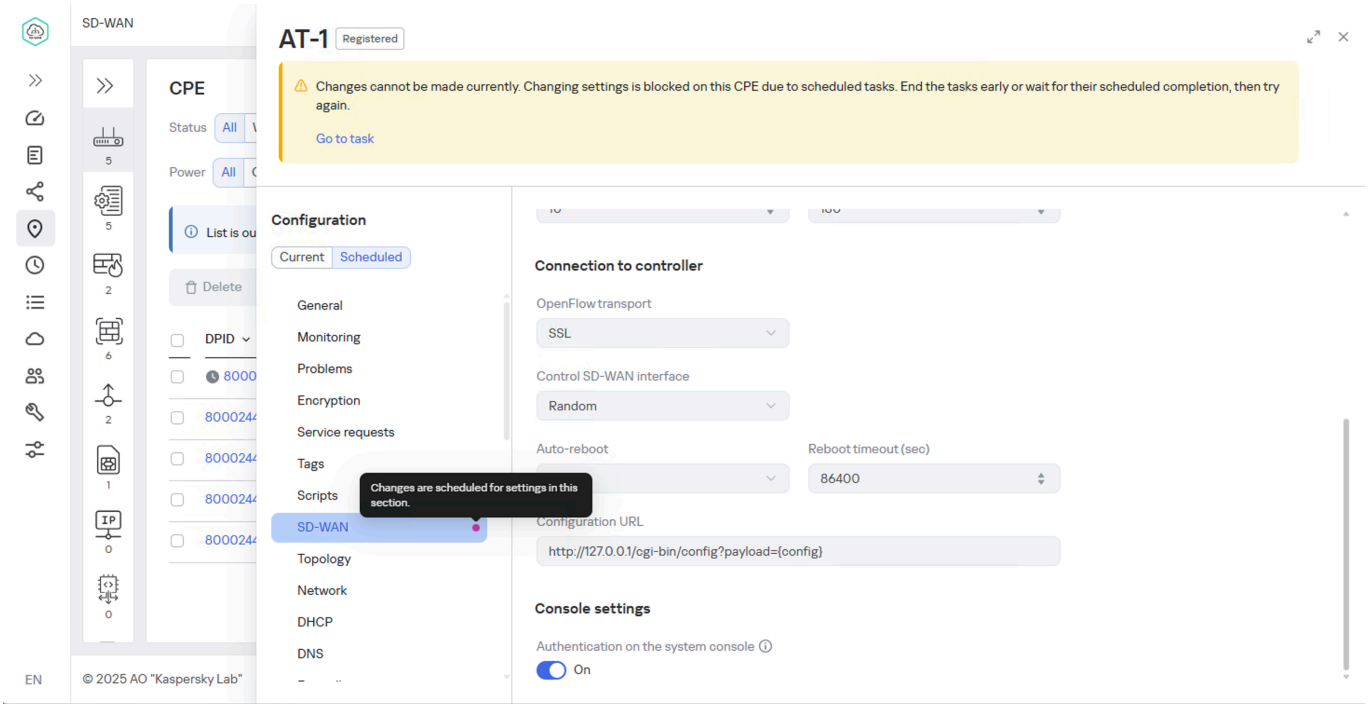
     2. No campo **Data de execução da tarefa programada**, insira a data e hora em que deseja executar a tarefa. A configuração padrão é a data e hora em que a tarefa começou a ser criada.

3. Se necessário, no campo **Nome da tarefa**, insira o nome da tarefa. Por padrão, o nome "Agendar atualização de configurações" é inserido nesse campo.

4. Clique em **Programação**.

Uma tarefa agendada para modificar as configurações do dispositivo CPE é criada. É possível visualizar o status da tarefa na tabela **Programador**.

O dispositivo CPE cujas alterações estão agendadas é exibido na tabela da seção **SD-WAN → CPE** com o ícone ao lado do DPID. Na área de configurações do dispositivo CPE, são exibidas novas guias que permitem visualizar a configuração atual e a configuração agendada do dispositivo. As seções com mudanças de configuração agendadas como parte de uma tarefa criada são realçadas visualmente. Não é possível editar nenhuma configuração do CPE ou de seu modelo de CPE até que a tarefa agendada seja concluída. É possível acessar a tarefa clicando em **Ir para a tarefa** e concluí-la antes da hora agendada ou excluí-la.



CPE exibido com as alterações agendadas

Excluir dispositivos CPE

Ao excluir um dispositivo CPE, todas as interfaces de serviço criadas nele são automaticamente excluídas.

Os dispositivos CPE excluídos não podem ser restaurados.

Para excluir dispositivos CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Para excluir um único dispositivo CPE:

   a. Clique no dispositivo CPE que deseja excluir.

      A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

   b. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

3. Para excluir vários dispositivos CPE:

   a. Marque a caixa de seleção ao lado dos dispositivos CPE que deseja excluir.

   b. Na parte superior da tabela, clique em **Ações** → **Excluir**.

4. Na janela de confirmação aberta, selecione o método de exclusão do dispositivo CPE:

   - **Excluir, anular registro e redefinir senha** para excluir o dispositivo CPE da interface da Web do orquestrador. Quando ligado, o dispositivo CPE se reconecta ao orquestrador e é exibido na interface da Web do orquestrador com o status **Desconhecido**.
   - **Redefinir as configurações padrão** para remover o dispositivo CPE da interface da Web do orquestrador e redefinir as configurações do dispositivo CPE para os padrões de fábrica. Quando ligado, o dispositivo CPE não se reconecta ao orquestrador e não é exibido na interface da Web do orquestrador.
   - **Forçar a exclusão** para excluir o dispositivo CPE da interface da Web do orquestrador. Selecione esta opção para remover um CPE indisponível ou uma entrada redundante da interface da Web do orquestrador.

5. Clique em **Excluir**.

Os dispositivos CPE são excluídos e não são mais exibidos na tabela.

Autenticação de dois fatores de um dispositivo CPE

É possível usar a *autenticação de dois fatores* para registrar o dispositivo CPE com segurança. Quando a autenticação de dois fatores está ativada, um token (chave de segurança) é registrado no banco de dados do orquestrador; esse token deve então ser colocado no dispositivo CPE ao registrá-lo usando a tecnologia Zero Touch Provisioning. O registro será bem-sucedido se, quando o dispositivo CPE estabelecer uma conexão automática com o orquestrador, o token no dispositivo corresponder ao token de CPE no banco de dados do orquestrador.

Não é possível usar a autenticação de dois fatores para um dispositivo CPE já registrado.

Para usar a autenticação de dois fatores para um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN**→ **CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE para o qual deseja usar a autenticação de dois fatores.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Ativação**.

   As configurações de autenticação de dois fatores são exibidas.

4. Na lista suspensa **Autenticação de dois fatores**, selecione **Ativado**. O valor padrão é **Desativado**.

5. Para gerar um novo token, clique em **Gerar** no campo **Token**.

6. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

Gerenciar certificados

Ao se comunicar com o orquestrador, o dispositivo CPE verifica se os certificados do orquestrador são confiáveis para impedir ataques MITM. Por padrão, o dispositivo CPE confia nas autoridades de certificação públicas.

Se o orquestrador usar certificados assinados por uma autoridade de certificação personalizada, carregue esses certificados na interface da Web do orquestrador e instale-os nos dispositivos CPE. Há suporte para certificados raiz independentes, bem como cadeias de certificados que consistem em um certificado raiz e vários certificados intermediários.

30 dias antes da expiração do certificado, uma notificação é exibida ao fazer login na interface da Web do orquestrador.

É possível visualizar a tabela de certificados na seção **SD-WAN** →**Certificados**. As informações sobre certificados são exibidas nas seguintes colunas da tabela:

- **Nome comum** é o nome de domínio ou nome do host para o qual o certificado é emitido.
- **Organização** é o nome da organização que emitiu o certificado.
- **Distribuir para CPEs** é a caixa de seleção para instalar o certificado em dispositivos CPE. Certificados com a caixa de seleção marcada são instalados nos dispositivos CPE nos seguintes casos:
  - Registro automático (ZTP) de um dispositivo CPE
  - Reinicialização do dispositivo CPE
  - Instalação manual de certificados no dispositivo CPE

  Selecionar certificados incorretamente pode fazer com que o dispositivo CPE pare de confiar no certificado do orquestrador e se desconecte dele.

- **De** é a data de início da validade do certificado.
- **Para** é a data de expiração do certificado.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Carregar um certificado usando a interface da Web do orquestrador

Para carregar um certificado na interface da Web do orquestrador:

1. No menu, acesse a seção **SD-WAN → Certificados**.

   Uma tabela de certificados é exibida.

2. Na parte superior da página, clique em **+ Certificado**.

3. Especifique o caminho para o arquivo de certificado no formato PEM. Tamanho máximo do arquivo: 16 KB.

   O certificado é carregado e exibido na tabela. A mensagem *Certificado <nome do certificado> carregado* é exibida.

Instalar certificados manualmente em dispositivos CPE

Para instalar certificados em dispositivos CPE:

1. No menu, vá para a seção **SD-WAN → Certificados**.

   Uma tabela de certificados é exibida.

2. Marque as caixas de seleção **Distribuir para CPEs** ao lado dos certificados carregados que deseja instalar nos dispositivos CPE.

3. Clique em **Aplicar a CPEs**.

   Os certificados são instalados nos dispositivos CPE. A mensagem *Os certificados foram aplicados a CPEs* é exibida.

Cenário: instalar certificados em um dispositivo CPE com firmware versão 23.07

É possível instalar um certificado raiz ou uma cadeia de certificados assinada por uma autoridade de certificação personalizada em um dispositivo CPE com firmware versão 23.07.

A versão 23.07 do firmware não é totalmente compatível com a versão atual do orquestrador, portanto, podem ocorrer problemas técnicos ao usar esta versão do firmware. Recomendamos atualizar o firmware de todos os dispositivos CPE para a versão mais recente.

O cenário para a instalação de certificados em dispositivos CPE com firmware versão 23.07 envolve as seguintes etapas:

1. **Carregar certificados usando a interface da Web do orquestrador**

   Carregue um certificado usando a interface da Web do orquestrador .

2. **Gerar uma URL com configurações básicas do dispositivo CPE**

   Gere uma URL com as configurações básicas do dispositivo CPE fazendo o seguinte:

   1. Na lista suspensa **Versão**, selecione **23.07**.

      São gerados endereços da Web de configuração para cada um dos certificados carregados.

   2. Clique em **Copiar** ao lado de todas as URLs geradas.

   3. Salve os endereços da Web copiados.

3. **Instalar certificados em um dispositivo CPE**

   Faça o seguinte:

   1. Conecte o dispositivo do administrador à porta LAN do dispositivo CPE.

      O dispositivo do administrador recebe um endereço IP e o endereço IP do gateway padrão via DHCP. O endereço IP do gateway padrão recebido é o endereço IP do dispositivo CPE.

   2. No dispositivo do administrador, acesse, um por um, cada endereço da Web gerado.

   O dispositivo CPE é reiniciado após a instalação de cada certificado. Observe que o dispositivo CPE pode obter um novo endereço IP após a reinicialização, portanto, pode ser necessário alterar o endereço da Web copiado anteriormente para instalar o próximo certificado.

Exportar um certificado

Para exportar um certificado:

1. No menu, vá para a seção **SD-WAN → Certificados**.

   Uma tabela de certificados é exibida.

2. Clique no certificado que deseja exportar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Exportar**.

Um arquivo de certificado no formato PEM é salvo no dispositivo local.

Excluir certificados

Os certificados excluídos não podem ser restaurados.

Para excluir certificados:

1. No menu, vá para a seção **SD-WAN → Certificados**.

   Uma tabela de certificados é exibida.

2. Para excluir um único certificado:

   a. Clique no certificado que deseja excluir

      A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

   b. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

3. Para excluir vários certificados:

   a. Marque as caixas de seleção ao lado dos certificados que deseja excluir.

   b. Na parte superior da tabela, clique em **Ações → Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

Os certificados são excluídos e não são mais exibidos na tabela.

Gerenciar diretórios APN

Para visualizar a tabela de diretórios APN, vá para a seção **SD-WAN → Modelos NetFlow** do menu. Por padrão, o diretório APN **DefaultAPNDir** é criado no portal do administrador.

As informações sobre diretórios APN são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do diretório APN.
- **Utilização** indica se o diretório APN está sendo usado por dispositivos CPE:
  - **Sim**.
  - **Não**.
- **Proprietário** é o locatário ao qual o diretório APN pertence.
- **Atualizado** é a data e hora em que as configurações do diretório APN foram modificadas pela última vez.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um diretório APN

Para criar um diretório APN:

1. No menu, acesse a seção **SD-WAN → Diretórios APN**.

   A tabela de diretórios APN é exibida.

2. Para adicionar um diretório APN manualmente:

   a. Na parte superior da página, clique em **+ Criar**.

      Isso abre a janela de adição de diretórios APN com uma tabela de registros de APN.

   b. No campo **Nome**, insira o nome do diretório APN.

   c. Adicione um ou mais registros APN clicando no botão **Adicionar**. Para cada registro, preencha os seguintes campos:

      - **PLMN** é o ID PLMN da operadora. Os três primeiros dígitos do ID PLMN são o MCC (Código de país móvel) e os dois ou três dígitos seguintes são o MNC (Código de rede móvel). Por exemplo, para a rede Vimpelcom no território russo, PLMN = 25099: MCC = 250 (Federação Russa), MNC = 99 (Vimpelcom).

        Configuração necessária.

      - **APN** é a string APN da operadora. Os caracteres permitidos são `[0-9A-Za-z-.]`. A string deve começar e terminar com uma letra ou um número. Pode ser uma string vazia. O comprimento máximo é de 100 caracteres.

        Configuração necessária.

      - **Nome de usuário de APN** é o nome de usuário do APN para autenticação com a operadora. Comprimento máximo: 32 caracteres. Os caracteres permitidos são `[0-9A-Za-z-._#$%*]`.

        Configuração opcional.

      - **Senha de APN** é a senha do APN para autenticação com a operadora. Comprimento máximo: 32 caracteres. Os caracteres permitidos são `[0-9A-Za-z~`!@#$%^&*()_-+={[}]|\:;"'<,>.?/]`.

        Configuração opcional.

      Para excluir um registro de APN, clique em **Excluir** ao lado dele.

   d. Clique em **Criar**.

3. Para adicionar o diretório APN a partir de um arquivo:

   a. Na parte superior da página, clique em **+ Upload a partir de arquivo**.

   b. Na janela aberta, selecione o arquivo JSON do qual deseja importar um diretório APN. O arquivo deve ter a seguinte estrutura:

```
{
 "name": "MyCustomDirectory",
 "entriesAmount": 150,
 "entries": [
 {"plmn": "25099", "apn": "internet.beeline.ru"},
 {"plmn": "25002", "apn": "internet"},
 {"plmn": "250201","apn": "some.private.apn","username": "apn-user","password": "********"}
 ]
}
```

O diretório APN é criado e exibido na tabela.

Exibir e redefinir sessões em dispositivos CPE

Os dispositivos CPE rastreiam e armazenam informações sobre conexões de entrada e de saída na forma de sessões. Uma sessão é um conjunto de atributos relacionados que permitem combinar pacotes individuais em uma entidade lógica e rastrear seu estado.

Você pode baixar e exibir a lista de sessões de um dispositivo CPE pela interface da Web do orquestrador, para diagnosticar rapidamente problemas de conexão, analisar a atividade da rede ou monitorar em tempo real o uso de recursos do CPE. Você também pode redefinir a lista de sessões em um dispositivo.

Para visualizar ou redefinir a lista de sessões em um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE para o qual deseja visualizar a lista de sessões.

3. A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

4. Vá para a seção Firewall e selecione a guia Sessões.

   A tabela de sessões é exibida. Por padrão, a tabela de sessões está vazia porque as sessões não foram baixadas do dispositivo CPE.

5. Solicite sessões do dispositivo clicando no botão **Solicitação do CPE**.

   Aguarde até que a lista de sessões seja recuperada do dispositivo CPE.

   As informações sobre as sessões são exibidas nas seguintes colunas da tabela:

   - **Protocolo**
   - **Tempo limite (s)**
   - **Estado**
   - **IP de origem**

- **Porta de origem**
- **IP de destino**
- **Porta de destino**
- **IP de origem da contraparte**
- **Porta de origem da contraparte**
- **IP de destino da contraparte**
- **Porta de destino da contraparte**
- **Pacotes de saída**
- **Pacotes de entrada**
- **Tráfego de saída (bytes)**
- **Tráfego de entrada (bytes)**
- **Flag da sessão**
- **Marcação**

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

6. Se você quiser filtrar as sessões exibidas na tabela:

   a. Clique no ícone de filtro próximo à borda direita do painel de ações acima da tabela.

   Isso abre a janela de criação de filtro.

   b. Adicione filtros para os campos necessários: para cada filtro, clique no botão **Adicionar**, selecione um campo e especifique um valor para filtrar.

   c. Aplique o filtro clicando no botão **Aplicar**.

   As sessões na tabela são filtradas.

7. Se você quiser redefinir a lista de sessões no dispositivo, clique no botão **Limpar sessões no CPE**.

   Um aviso é exibido:

   A limpeza de sessões pode causar a perda temporária da conexão com o controlador, restabelecendo os links deste CPE e, como consequência, a perda temporária do tráfego.

   Confirme a redefinição das sessões clicando em **Limpar a tabela de sessão**.

Excluir e desativar dispositivos CPE automaticamente

No modelo de CPE ou no dispositivo CPE, é possível especificar após quanto tempo o dispositivo CPE será excluído ou desativado se a sessão de gerenciamento com o controlador for encerrada. Ambas as funções são usadas para impedir o roubo de dispositivos CPE. A função de exclusão automática também é usada para limpar entradas obsoletas da interface da Web do orquestrador. Ambas as funções estão desativadas por padrão.

O tempo de exclusão ou desativação automática especificado em um modelo de CPE é aplicado automaticamente a todos os dispositivos CPE que usam o modelo.

Para configurar a exclusão e desativação automáticas de dispositivos CPE:

1. Configure a exclusão e desativação automáticas de uma das seguintes formas:

   - Para configurar a exclusão e desativação automáticas em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Desativação**.

   - Para configurar a exclusão e desativação automáticas em um dispositivo CPE, vá para a seção **SD-WAN**→ **CPE** do menu, clique no dispositivo CPE, selecione a guia **Desativação** e marque as caixas de seleção **Substituir**.

   As configurações de exclusão e desativação automáticas do dispositivo CPE são exibidas.

2. Ative a exclusão automática do dispositivo CPE:

   a. Marque a caixa de seleção **Ativar** ao lado do campo **Tempo limite de exclusão (s)**.

   b. No campo **Tempo limite de exclusão (s)**, insira o tempo em segundos após o qual o dispositivo CPE será excluído se a comunicação com o controlador não for possível. Intervalo de valores: 60 a 31.536.000. O valor inserido não pode ser menor que o valor especificado para a desativação automática.

3. Ative a desativação automática do dispositivo CPE:

   a. Marque a caixa de seleção **Ativar** ao lado do campo **Tempo limite de desativação (s)**.

   b. No campo **Tempo limite de desativação (s)**, insira o tempo em segundos após o qual o dispositivo CPE será desativado se a comunicação com o controlador não for possível. Intervalo de valores: 60 a 31.536.000. O valor inserido não pode ser maior que o valor especificado para a exclusão automática.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Agrupar dispositivos CPE usando tags

As *tags* descrevem as configurações do dispositivo CPE, como modelo, versão do firmware e endereço do local. Quando um dispositivo CPE é adicionado, tags são automaticamente atribuídas a ele, descrevendo seu modelo e o locatário ao qual o dispositivo CPE foi adicionado.

As tags podem ser usadas para agrupar dispositivos CPE e executar ações em grupos. Por exemplo, é possível atribuir a mesma tag a dispositivos CPE que estão no mesmo local e, em seguida, atualizar o firmware em todos eles.

Para ter uma tag atribuída, o dispositivo CPE deve ter o status **Registrado**. Duas tags idênticas não podem ser atribuídas ao mesmo dispositivo CPE.

Atribuir uma tag a dispositivos CPE

Para atribuir uma tag a dispositivos CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Para atribuir uma tag a um único dispositivo CPE:

   a. Clique no dispositivo CPE ao qual deseja atribuir uma tag.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

   b. Selecione a guia **Tags**.

   As tags atribuídas são exibidas.

   c. Insira a tag e clique no ícone de atribuição +.

   d. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

3. Para atribuir uma tag a vários dispositivos CPE:

   a. Marque as caixas de seleção ao lado dos dispositivos CPE aos quais deseja atribuir uma tag.

   b. Na parte superior da tabela, clique em **Ações → Atribuir tags**.

   c. Na janela aberta, insira a tag e clique no ícone de atribuição +.

   d. Clique em **Adicionar**.

A tag é atribuída aos dispositivos CPE.

Remover uma tag de dispositivos CPE

Para remover uma tag de dispositivos CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Para remover uma tag de um único dispositivo CPE:

    a. Clique no dispositivo CPE do qual deseja remover uma tag.

    A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

    b. Selecione a guia **Tags**.

    As tags atribuídas são exibidas.

    c. Clique no ícone remover ✕ ao lado da tag que deseja remover.

    d. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

3. Para remover uma tag de vários dispositivos CPE:

    a. Marque as caixas de seleção ao lado dos dispositivos CPE dos quais deseja remover uma tag.

    b. Na parte superior da tabela, clique em **Ações** → **Excluir tags**.

    c. Na janela aberta, remova as tags de uma das seguintes formas:

    - Clique no ícone remover ✕ ao lado da tag que deseja remover.
    - Insira a tag que deseja remover e selecione-a na lista suspensa.

    d. Clique em **Excluir**.

A tag do dispositivo CPE é removida.

Configurar registros em dispositivos CPE

Os logs gerados em dispositivos CPE são armazenados localmente ou enviados para um servidor syslog externo. Ao armazenar logs localmente, é possível especificar um tamanho máximo. É possível especificar um prefixo a ser atribuído aos logs antes que sejam enviados ao servidor syslog externo.

Para visualizar o log local no dispositivo CPE, solicite informações de diagnóstico.

É possível especificar as configurações de logs em um modelo de CPE ou no dispositivo CPE. As configurações de logs especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para configurar logs em dispositivos CPE:

1. Se quiser que o dispositivo CPE envie registros para um servidor syslog externo em formato criptografado, primeiro carregue o certificado CA do servidor syslog no dispositivo CPE:

    1. Abra a guia **SD-WAN** →**Certificados**, clique em **+Adicionar** e, no formulário exibido, clique em **Carregar** e selecione o arquivo de certificado.

    O certificado carregado aparece na tabela de certificados.

2. Na tabela de certificados, marque a caixa de seleção **Distribuir para CPEs** para o certificado adicionado.

3. Clique em **Aplicar a CPEs**.

2. Configure os logs de uma das seguintes formas:

   - Para configurar logs em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu e clique no modelo de CPE; na área de configurações exibida, selecione a seção **Registro** e, na área de configurações, selecione a guia **Geral**.

   - Para configurar registros em um dispositivo CPE, acesse a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a seção **Registro**; na área de configurações, selecione a guia **Geral** e ative o botão de alternância **Substituir**.

   As configurações de logs são exibidas.

3. No campo **IP/FQDN**, insira o endereço IP ou o nome de domínio totalmente qualificado do servidor syslog.

   Se quiser usar uma conexão criptografada para enviar mensagens syslog e o certificado CA correspondente tiver sido emitido para um nome de domínio, no campo IP/FQDN, especifique o nome de domínio totalmente qualificado (FQDN). Esse nome de domínio deve ser resolvido por meio do servidor DNS especificado ao configurar o DNS no dispositivo CPE.

4. No campo **Porta**, insira o número da porta do servidor syslog. Intervalo de valores: 0 a 65.353.

5. Na lista suspensa Protocolo, selecione o protocolo para o envio de registros para o servidor syslog:

   - **UDP**. Essa é a configuração padrão.

   - **TCP.**

   - **TLS**. Selecione esta opção se desejar que o dispositivo CPE envie registros para o servidor syslog externo em formato criptografado.

     Os parâmetros do algoritmo de criptografia (cifra) para a comunicação entre o cliente e o servidor syslog são determinados pelo servidor syslog. As seguintes versões de cifras e de TLS são compatíveis com dispositivos CPE:

     - `TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD`
     - `TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any Au=any Enc=CHACHA20/POLY1305(256) Mac=AEAD`
     - `TLS_AES_128_GCM_SHA256 TLSv1.3 Kx=qualquer Au=qualquer Enc=AESGCM(128) Mac=AEAD`
     - `ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD`
     - `ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD`
     - `ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD`
     - `ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD`
     - `DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD`

6. No campo **Tamanho do arquivo (KB)**, insira o tamanho máximo dos registros no dispositivo CPE em quilobytes. Intervalo de valores: 64 a 2048. O valor padrão é 64. Se o tamanho máximo do log for excedido, logs novos substituem os mais antigos.

7. Se você quiser que o dispositivo CPE adicione um prefixo aos registros, especifique o prefixo no campo **Prefixo do nome do arquivo**. O comprimento máximo do prefixo é de 256 caracteres.

8. Se necessário, configure a filtragem de mensagens enviadas ao servidor syslog usando o campo **Filtrar mensagens**. Quando um filtro de mensagem é usado, somente os registros que contêm as strings especificadas no filtro são enviados ao servidor syslog. Você pode especificar até dez strings individuais. As strings são combinadas com o conectivo lógico OU. Caracteres permitidos para strings de filtro:

   - Letras latinas maiúsculas (A–Z)
   - Letras latinas minúsculas (a–z)
   - Algarismos (0–9)
   - Caracteres especiais : - . _
   - O caractere de espaço

9. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar modems

Esta funcionalidade não é compatível com alguns modelos. Entre em contato com o Suporte Técnico da Kaspersky.

Um dispositivo CPE pode ter até quatro modems para estabelecer conexão com a rede celular. Para visualizar a tabela de modems, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Modems**. As informações sobre modems são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do modem.
- **Endereço IP** é o endereço IP do modem.
- **Sub-rede** é a sub-rede à qual o modem está conectado.
- **Gateway** é o gateway ao qual o modem está conectado.
- **DNS 1**, **DNS 2** são servidores DNS usados pelo modem.
- **Sinal** é a intensidade do sinal do modem.
- **Formato de data** é o protocolo de transferência de dados do modem.
- **Registro** é o status de registro do modem.
- **Rede** é a rede à qual o modem está conectado.

- **País** é o país onde o modem está registrado.
- **PLMN MCC** é o Código de país móvel.
- **PLMN MNC** é o Código de rede móvel.
- **Roaming** indica se roaming está sendo usado no modem:
  - **Sim**.
  - **Não**.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Atualizar o firmware

As novas versões do software do dispositivo CPE são distribuídas pela Kaspersky na forma de um firmware. Firmwares baseado nos seguintes switches de software são compatíveis:

- Open vSwitch (OVS) é uma implementação de switch de software com processamento de pacotes no nível do kernel. Esse tipo de switch é adequado para a maioria dos dispositivos e é selecionado por padrão.
- O Switch Operating System (SWOS) é uma implementação alternativa de switch de software com processamento de pacotes baseado em DPDK. Pode oferecer maior desempenho graças ao processamento de pacotes com bypass do kernel.

Um arquivo TAR.GZ com o firmware pode ser baixado no diretório /cpe do kit de distribuição.

É possível atualizar o firmware em um dispositivo CPE de três maneiras:

- Atualizar o firmware do dispositivo CPE manualmente sem usar a interface da Web do orquestrador.
- Agendar atualizações de firmware em dispositivos CPE selecionados. Nesse caso, carregue o firmware para a interface da Web do orquestrador, selecione os dispositivos CPE nos quais deseja atualizar o firmware e, em seguida, atualize o firmware. Uma tarefa de atualização de firmware é criada automaticamente no agendador de tarefas.
- Agendar atualizações de firmware em dispositivos CPE com tags específicas. Nesse caso, carregue o firmware para a interface da Web do orquestrador, atribua tags aos dispositivos CPE nos quais deseja atualizar o firmware e, em seguida, crie uma tarefa de atualização de firmware no agendador de tarefas. Ao criar a tarefa, é necessário especificar as tags atribuídas aos dispositivos CPE.

O dispositivo CPE é reiniciado durante o processo de atualização do firmware.

É possível visualizar a tabela de firmwares carregados para a interface da Web na seção **SD-WAN→ Firmware**. As informações sobre firmware são exibidas nas seguintes colunas da tabela:

- **Versão** é a versão do firmware.
- **Tamanho (MB)** é o tamanho do arquivo de firmware em megabytes.

- **SHA256** é o hash do firmware.
- **Arquitetura** é a arquitetura do conjunto de instruções (ISA) do firmware.
- **Data de lançamento** é a data de lançamento do firmware.
- **Modelo** é o modelo dos dispositivos CPE com os quais o firmware é compatível.
- **Tipo de switch** é o tipo de switch de software no qual o firmware é baseado (OVS ou SWOS).

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Atualizar manualmente o firmware em um dispositivo CPE

Ao seguir estas etapas, será solicitado que você insira as credenciais do dispositivo CPE. Após o registro, a senha padrão do dispositivo CPE é alterada automaticamente. É possível visualizar a senha do dispositivo CPE na interface da Web do orquestrador.

Para atualizar manualmente o firmware em um dispositivo CPE:

1. Baixe o arquivo de firmware do diretório /cpe do kit de distribuição para o dispositivo do administrador, por exemplo, seu laptop. Caso não saiba qual versão de firmware instalar no dispositivo CPE, use a tabela de correspondência de modelos de dispositivo CPE com versões de firmware.
2. Conecte o dispositivo do administrador à porta LAN do dispositivo CPE.

   O dispositivo do administrador recebe o endereço IP do gateway padrão via DHCP. O endereço IP do gateway padrão recebido é o endereço IP do dispositivo CPE.
3. Conecte-se ao dispositivo CPE por meio de SCP, por exemplo, usando o WinSCP. Para estabelecer uma conexão por SCP, especifique o endereço IP e insira as credenciais do dispositivo CPE.
4. Coloque o arquivo comprimido do firmware no diretório /tmp.
5. Conecte-se ao dispositivo CPE através de uma conexão SSH. Para estabelecer uma conexão por SSH, especifique o endereço IP e insira as credenciais do dispositivo CPE.
6. Mude para o diretório /tmp:

   ```
   cd /tmp/
   ```
7. Atualize o firmware no dispositivo CPE de uma das seguintes formas:

   - Para manter as configurações do dispositivo CPE inalteradas após atualizar o firmware, execute o seguinte comando:

     ```
     sysupgrade knaas-<nome do arquivo comprimido do firmware>
     ```
   - Para restaurar o dispositivo CPE para as configurações de fábrica após atualizar o firmware, execute o seguinte comando:

     ```
     sysupgrade -n knaas-cpe<nome do arquivo comprimido do firmware>
     ```

Quando um dispositivo CPE é restaurado para as configurações de fábrica, ele é desconectado do orquestrador. Para reconectar o dispositivo CPE ao orquestrador, é necessário registrar automaticamente (ZTP) o dispositivo CPE.

A nova versão do firmware é instalada no dispositivo CPE e, em seguida, o dispositivo CPE é reiniciado. Por padrão, o endereço IP do dispositivo CPE permanece inalterado e o DHCP é ativado nas portas LAN.

Carregar firmwares para a interface da Web do orquestrador

Para carregar firmwares na interface da Web do orquestrador:

1. Baixe arquivo comprimido de firmware do diretório /cpe do kit de distribuição para o dispositivo local. Caso não saiba qual versão de firmware instalar no dispositivo CPE, use a tabela de correspondência de modelos de dispositivo CPE com versões de firmware.

2. No menu, acesse a seção **SD-WAN → Firmware**.

   Uma tabela de firmwares é exibida.

3. Na parte superior da página, clique em **+ Firmware**.

4. Insira o caminho para o arquivo de firmware. Ao especificar um caminho, é possível selecionar vários arquivos comprimidos ao mesmo tempo.

O firmware é carregado e exibido na tabela.

Agendar atualizações de firmware em dispositivos CPE selecionados

Para criar uma tarefa de atualização de firmware agendada em dispositivos CPE selecionados:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Prossiga com a atualização de firmware agendada de uma das seguintes formas:

   - Para executar uma atualização de firmware agendada em um único dispositivo CPE, clique no dispositivo CPE para abrir a janela de propriedades do dispositivo; nessa janela, abra o menu de ação clicando no ícone ⋮ no canto superior direito e selecione **Atualizar firmware**.

   - Para executar uma atualização de firmware agendada em vários dispositivos CPE, marque as caixas de seleção ao lado dos dispositivos relevantes e, na parte superior da tabela, clique em **Ações → Atualizar firmware**.

   O firmware obsoleto é destacado em laranja na coluna **Versão do SW** da tabela de dispositivos CPE. Também é possível encontrar dispositivos CPE com versões de firmware desatualizadas usando o filtro **Atualização necessária** na parte superior da tabela.

3. Na janela aberta, no campo **Nome da tarefa**, insira o nome da tarefa agendada.

4. Use o botão **Tipo de switch** para selecionar o tipo de switch de software para o novo firmware (OVS ou SWOS).

   Caso esteja atualizando o firmware em vários dispositivos CPE ao mesmo tempo, selecione o tipo de switch de software para que corresponda ao firmware de todos os dispositivos selecionados. Se o tipo de firmware em pelo menos um dispositivo não corresponder ao tipo de switch de software selecionado, a mensagem **O CPE só pode ser atualizado com firmware com o mesmo tipo de switch** será exibida na janela de criação da tarefa de atualização do firmware e a tarefa não poderá ser criada. Caso esteja atualizando o firmware em um único dispositivo, o aviso **O tipo de switch selecionado não corresponde ao tipo de switch do CPE. Isso pode levar o dispositivo a ficar inacessível após a atualização de firmware devido a possíveis inconsistências de configuração** é exibido ao selecionar um tipo de switch incompatível, mas é possível criar a tarefa.

   Não recomendamos atualizar o firmware para uma versão baseada em um tipo de switch de software diferente.

5. Na lista suspensa **Versão**, selecione a versão do firmware carregado. A lista exibe as versões de firmware que correspondem ao tipo de switch de software selecionado na configuração **Tipo de switch**. Caso não saiba qual versão de firmware instalar no dispositivo CPE, use a tabela de correspondência de modelos de dispositivo CPE com versões de firmware.

   Se a lista não tiver nenhuma versão de firmware correspondente (nenhuma versão foi encontrada para corresponder ao tipo de switch de software selecionado ou nenhuma versão foi carregada no orquestrador), a mensagem **Nenhum firmware disponível para os CPEs selecionados. É possível carregar um novo firmware** é exibida na parte superior da janela com um link para a seção **SD-WAN→ Firmware**.

6. No campo **Data de execução da tarefa programada**, insira a data e hora em que deseja executar a tarefa. Por padrão, a data e hora especificadas são a data e hora em que você começou a criar a tarefa.

7. Para restaurar o dispositivo CPE para as configurações de fábrica após atualizar o firmware, desmarque a caixa de seleção **Salvar configurações de CPE**. Se a caixa de seleção estiver marcada, as configurações existentes do dispositivo CPE não serão modificadas após uma atualização de firmware. Esta caixa de seleção é selecionada por padrão.

   Quando um dispositivo CPE é restaurado para as configurações de fábrica, ele é desconectado do orquestrador. Para reconectar o dispositivo CPE ao orquestrador, é necessário registrar automaticamente (ZTP) o dispositivo CPE.

8. A caixa de seleção **Forçar atualização** permite forçar a atualização do firmware, mesmo se a verificação interna do CPE mostrar que o novo firmware é incompatível com o antigo. Esta caixa de seleção está desmarcada por padrão.

9. Clique em **Next**.

   Duas tabelas de dispositivos CPE são exibidas. O firmware dos dispositivos CPE na tabela superior será atualizado. O firmware dos dispositivos CPE na tabela inferior não será atualizado. As informações sobre dispositivos CPE são exibidas nas seguintes colunas da tabela:

   - **DPID** é o DPID do dispositivo CPE.
   - **Modelo** é o modelo do dispositivo CPE.
   - **Tipo de switch** é o tipo de switch de software do firmware do dispositivo CPE (OVS ou SWOS).
   - **Nome** é o nome do dispositivo CPE.
   - **Versão do SW** é a versão do firmware do dispositivo CPE.

- **Locatário** é o locatário ao qual o dispositivo CPE foi adicionado.
- **Motivo** é o motivo por que o firmware não pode ser atualizado. Essa coluna é exibida apenas na tabela inferior.

Se a tabela superior contiver dispositivos CPE cujo firmware você não deseja atualizar, é possível migrá-los para a tabela inferior.

10. Clique em **Programação**.

A tarefa de atualização do firmware é criada e exibida na tabela de tarefas. O status das tarefas é exibido na coluna **Status**. Se a tarefa de atualização de firmware for concluída com êxito, seu status será alterado para **Concluído**.

Agendar atualizações de firmware em dispositivos CPE com tags específicas

Para criar uma tarefa de atualização de firmware agendada em dispositivos CPE com tags específicas:

1. No menu, acesse a seção **Programador**.

   A tabela de tarefas é exibida.

2. Na parte superior da página, clique em **+ Tarefa**.
3. Na janela aberta, na lista suspensa **Tipo**, selecione **Atualização de firmware**.
4. No campo **Nome da tarefa**, insira o nome da tarefa.
5. Use o botão **Tipo de switch** para selecionar o tipo de switch de software para o novo firmware (OVS ou SWOS).
6. Na lista suspensa **Versão**, selecione a versão do firmware carregado. A lista exibe as versões de firmware que correspondem ao tipo de switch de software selecionado na configuração **Tipo de switch**. Caso não saiba qual versão de firmware instalar no dispositivo CPE, use a tabela de correspondência de modelos de dispositivo CPE com versões de firmware.

   Se a lista não tiver nenhuma versão de firmware correspondente (nenhuma versão foi encontrada para corresponder ao tipo de switch de software selecionado ou nenhuma versão foi carregada no orquestrador), a mensagem **Nenhum firmware disponível para os CPEs selecionados. É possível carregar um novo firmware** é exibida na parte superior da janela com um link para a seção **SD-WAN→ Firmware**.

7. No campo **Data de execução da tarefa programada**, insira a data e hora em que deseja executar a tarefa. Por padrão, a data e hora especificadas são a data e hora em que você começou a criar a tarefa.
8. Para restaurar o dispositivo CPE para as configurações de fábrica após atualizar o firmware, desmarque a caixa de seleção **Salvar configurações de CPE**. Se a caixa de seleção estiver marcada, as configurações existentes do dispositivo CPE não serão modificadas após uma atualização de firmware. Esta caixa de seleção é selecionada por padrão.

   Quando um dispositivo CPE é restaurado para as configurações de fábrica, ele é desconectado do orquestrador. Para reconectar o dispositivo CPE ao orquestrador, é necessário registrar automaticamente (ZTP) o dispositivo CPE.

9. A caixa de seleção **Forçar atualização** permite forçar a atualização do firmware, mesmo se a verificação interna do CPE mostrar que o novo firmware é incompatível com o antigo. Esta caixa de seleção está desmarcada por padrão.

10. No campo **Tags**, insira as tags atribuídas aos dispositivos CPE nos quais deseja atualizar o firmware. O firmware obsoleto é destacado em laranja na coluna **Versão do SW** da tabela de dispositivos CPE. Também é possível encontrar dispositivos CPE com versões de firmware desatualizadas usando o filtro **Atualização necessária** na parte superior da tabela.

11. Clique em **Next**.

    Duas tabelas de dispositivos CPE são exibidas. O firmware dos dispositivos CPE na tabela superior será atualizado. O firmware dos dispositivos CPE na tabela inferior não será atualizado. As informações sobre dispositivos CPE são exibidas nas seguintes colunas da tabela:

    - **DPID** é o DPID do dispositivo CPE.
    - **Modelo** é o modelo do dispositivo CPE.
    - **Tipo de switch** é o tipo de switch de software do firmware do dispositivo CPE (OVS ou SWOS).
    - **Nome** é o nome do dispositivo CPE.
    - **Versão do SW** é a versão do firmware do dispositivo CPE.
    - **Locatário** é o locatário ao qual o dispositivo CPE foi adicionado.
    - **Motivo** é o motivo por que o firmware não pode ser atualizado. Essa coluna é exibida apenas na tabela inferior.

    Se a tabela superior contiver dispositivos CPE cujo firmware você não deseja atualizar, é possível migrá-los para a tabela inferior.

12. Clique em **Criar**.

    A tarefa de atualização do firmware é criada e exibida na tabela. O status das tarefas é exibido na coluna **Status**. Se a tarefa de atualização de firmware for concluída com êxito, seu status será alterado para **Concluído**.

Restaurar o firmware de um dispositivo CPE KESR-M1

É possível restaurar o firmware e redefinir um dispositivo CPE KESR-M1 para as configurações de fábrica caso tenha perdido as credenciais do CPE ou encontre um problema com o firmware.

Quando um dispositivo CPE é restaurado para as configurações de fábrica, ele é desconectado do orquestrador. Para reconectar o dispositivo CPE ao orquestrador, é necessário registrar automaticamente (ZTP) o dispositivo CPE.

Para restaurar o firmware de um dispositivo CPE KESR-M1:

1. Baixe o arquivo de firmware do diretório /cpe do kit de distribuição para o dispositivo do administrador, por exemplo, seu laptop. Caso não saiba qual versão de firmware instalar no dispositivo CPE, use a tabela de correspondência de modelos de dispositivo CPE com versões de firmware.

2. Extraia o arquivo de firmware para obter o firmware no formato BIN.

3. Ligue o dispositivo CPE com o firmware de fábrica:

   a. Desconecte o cabo de alimentação do dispositivo CPE.

   b. Conecte o cabo de alimentação e mantenha pressionado o botão **RESET** no dispositivo CPE por 10 segundos.

   O dispositivo CPE é ligado com o firmware de fábrica.

4. Conecte o dispositivo do administrador à porta LAN do dispositivo CPE.

   O dispositivo do administrador obtém um endereço IP e o endereço IP do gateway padrão na sub-rede 192.168.1.0/24 via DHCP.

5. Na barra de endereço do navegador no dispositivo do administrador, insira `192.168.1.1` e pressione **Enter**.

   Isso abre a página de upload do firmware do dispositivo CPE.

6. Clique no botão de upload do firmware e especifique o caminho para o firmware no formato BIN. O firmware no formato BIN foi obtido na etapa 2 destas instruções.

A nova versão do firmware é instalada no dispositivo CPE e, em seguida, o dispositivo CPE é reiniciado. Por padrão, o endereço IP do dispositivo CPE é 192.168.7.1 e o DHCP é ativado nas portas LAN.

Restaurar o firmware de um dispositivo CPE KESR-M2-5

É possível restaurar o firmware e redefinir um dispositivo CPE KESR-M2-5 para as configurações de fábrica caso tenha perdido as credenciais do CPE ou encontre um problema com o firmware.

Quando um dispositivo CPE é restaurado para as configurações de fábrica, ele é desconectado do orquestrador. Para reconectar o dispositivo CPE ao orquestrador, é necessário registrar automaticamente (ZTP) o dispositivo CPE.

Para restaurar o firmware de um dispositivo CPE KESR-M2-5:

1. Baixe o arquivo de firmware do diretório /cpe do kit de distribuição para o dispositivo do administrador, por exemplo, seu laptop. Caso não saiba qual versão de firmware instalar no dispositivo CPE, use a tabela de correspondência de modelos de dispositivo CPE com versões de firmware.

2. Extraia o arquivo de firmware para obter um arquivo no formato IMG.GZ.

3. Descompacte o arquivo IMG.GZ para obter a imagem do firmware no formato IMG.

4. Use o firmware IMG para criar uma unidade USB inicializável usando um software de gravação de imagem de disco, como o BalenaEtcher.

5. Conecte o dispositivo do administrador ao dispositivo CPE com um cabo do console e insira a unidade USB na porta USB do dispositivo CPE.

6. Especifique as configurações para estabelecer uma sessão do console com o dispositivo CPE no dispositivo do administrador, por exemplo, usando o aplicativo PuTTY, e faça o seguinte:

   - Especifique o número da porta de comunicações (porta COM) do dispositivo do administrador.
   - Especifique `115200` como a velocidade da sessão.

7. Desconecte e reconecte o cabo de alimentação do dispositivo CPE. Pressione **F7** ou **F11** enquanto o dispositivo CPE estiver sendo ligado.

8. No menu que se abre, selecione a unidade USB e pressione **Enter**.

   O dispositivo CPE é inicializado a partir da unidade USB.

9. Conecte o dispositivo do administrador à porta LAN do dispositivo CPE.

   O dispositivo do administrador obtém um endereço IP e o endereço IP do gateway padrão na sub-rede 192.168.7.0/24 via DHCP.

10. Conecte-se ao dispositivo CPE através de SCP, por exemplo, usando o WinSCP. Para estabelecer uma conexão por SCP, especifique o endereço IP e insira as credenciais padrão do dispositivo CPE.

11. Coloque o firmware no formato IMG no diretório /tmp.

12. Conecte-se ao dispositivo CPE por meio de SSH ou estabeleça uma sessão do console com o dispositivo CPE. Para estabelecer uma conexão por SSH ou iniciar uma sessão do console, especifique o endereço IP e insira as credenciais padrão do dispositivo CPE.

13. Mude para o diretório /tmp:

    ```
    cd /tmp/
    ```

14. Copie a imagem do firmware no formato IMG para /dev/sda:

    ```
    dd if=< nome do arquivo IMG do firmware > bs=1M of=/dev/sda
    ```

15. Reinicie o dispositivo CPE executando o seguinte comando:

    ```
    reboot
    ```

A nova versão do firmware é instalada no dispositivo CPE e, em seguida, o dispositivo CPE é reiniciado. Por padrão, o endereço IP do dispositivo CPE é 192.168.7.1 e o DHCP é ativado nas portas LAN.

Correspondência de modelos de dispositivo CPE com versões de firmware

A tabela abaixo mostra a correspondência de modelos de dispositivo CPE com as versões de firmware compatíveis.

Modelo do dispositivo CPE	Arquivo de firmware
KESR M1 (V1 TTK)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.firmware.kesr-m1-r-5g-1l-w-v1-ttk_en-US_ru-RU.tar.gz
KESR M1 (V2)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.firmware.kesr-m1-r-5g-2l-w-v2_en-US_ru-RU.tar.gz

Modelo do dispositivo CPE	Arquivo de firmware
KESR M1 (V3)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.efi.amd64-kesr-m1-k-4g-2l-w-v3_en-US_ru-RU.tar.gz
KESR M2 (Wi-Fi/LTE)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.efi.amd64-kesr-m2-k-5g-1l-w_en-US_ru-RU.tar.gz
KESR M2 (SFP)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.efi.amd64-kesr-m2-k-5g-1s_en-US_ru-RU.tar.gz
KESR M3	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.efi.amd64-kesr-m3-k-4g-4s_en-US_ru-RU.tar.gz
KESR M4 (SFPx2)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.efi.amd64-kesr-m4-k-4g-2x_en-US_ru-RU.tar.gz
KESR M4 (SFPx4/RJ-45x8)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.efi.amd64-kesr-m4-k-8g-4x_en-US_ru-RU.tar.gz
KESR M5 (SFPx8)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.efi.amd64-kesr-m5-k-4g-8x_en-US_ru-RU.tar.gz
KESR M5 (SFPx4/RJ-45x8)	knaas-cpe_<versão do firmware>.release.<número da versão da solução>.efi.amd64-kesr-m5-k-8g-4x_en-US_ru-RU.tar.gz

Excluir o firmware

Não é possível excluir um firmware que esteja sendo usado em pelo menos uma tarefa. Para excluir um firmware sendo usado em tarefas, primeiro exclua as tarefas.

O firmware excluído não pode ser restaurado.

Para excluir um firmware:

1. No menu, acesse a seção **SD-WAN** → **Firmware**.

   Uma tabela de firmwares é exibida.

2. Marque as caixas de seleção ao lado do firmware que deseja excluir.

3. Na parte superior da tabela, clique em **Ações** → **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

   O firmware é excluído e não é mais exibido na tabela.

Configuração adicional de dispositivos CPE usando scripts

É possível usar scripts para a configuração adicional de dispositivos CPE. Também é possível adicionar scripts a um modelo de CPE. Os scripts adicionados ao modelo de CPE são automaticamente adicionados a todos os dispositivos CPE que usam o modelo. Os scripts adicionados podem ser executados automaticamente ou manualmente. Os scripts são executados automaticamente quando as condições especificadas nas configurações do script são satisfeitas, por exemplo, quando um dispositivo CPE é registrado.

A execução de scripts é responsabilidade do VNFM, portanto, a conexão de rede entre o VNFM e os dispositivos CPE deve ser garantida antes de começar a trabalhar com scripts. Por padrão, o número da porta para conectar o VNFM ao dispositivo e o nome de usuário para executar scripts são especificados no modelo de CPE. Altere o número da porta e o nome de usuário, se necessário.

É possível visualizar a tabela de scripts em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de scripts em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Scripts**.
- Para visualizar a tabela de scripts em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Scripts**.

As informações sobre scripts são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do script.
- **Executor** é o interpretador.
- **Autenticação** é o tipo de autenticação VNFM no dispositivo CPE.
- **Executor personalizado** é o caminho para o interpretador personalizado.
- **Tempo limite (s)** é o tempo em segundos após o qual o VNFM para de tentar executar um script que não pôde ser executado na primeira vez.
- **Repetir execução** indica se o script pode ser executado novamente:
  - **Sim**.
  - **Não**.
- **Estágio** é o estágio da operação do dispositivo CPE no qual o VNFM executa o script.
- **Script** é o nome do arquivo de script ou do manual do Ansible.
- **Arquivo** é o nome do arquivo comprimido com arquivos adicionais que o script precisa para ser executado.
- **Ações** contém as ações que podem ser executadas com o script.

Adicionar um script a dispositivos CPE

É possível adicionar um script a um modelo de CPE. Os scripts adicionados ao modelo de CPE são automaticamente adicionados a todos os dispositivos CPE que usam o modelo.

Para adicionar um script a dispositivos CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE ao qual deseja adicionar um script.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Selecione a guia **Scripts**.

   Isso exibirá o número da porta que o VNFM usa para estabelecer a conexão com o dispositivo CPE, o nome de usuário para execução de scripts e a tabela de scripts se pelo menos um script tiver sido adicionado.

4. Clique em **+ Script**.

5. Na janela aberta, no campo **Nome**, insira o nome do script. O comprimento máximo do nome é de 255 caracteres.

6. No campo **Tempo limite (s)**, insira o tempo em segundos após o qual o VNFM para de tentar executar um script que não pôde ser executado na primeira vez. O valor padrão é `360`.

7. Na lista suspensa **Executor**, selecione um dos seguintes valores:

   - **Ansible**. Essa é a configuração padrão.
   - **Shell**
   - **Expect**
   - Personalizado para usar um interpretador no dispositivo CPE. Se esse valor for selecionado, insira o caminho para o interpretador personalizado no campo **Executor personalizado**.

8. Na lista suspensa **Estágio**, selecione em qual estágio da operação do dispositivo CPE o VNFM executa o script:

   - **Registro**. Essa é a configuração padrão.
   - **Exclusão**
   - **Manualmente** para executar o script apenas manualmente.

9. Caso precise executar o script novamente, marque a caixa de seleção **Repetir execução**. Esta caixa de seleção está desmarcada por padrão. Considerações especiais para executar um script novamente:

   - Caso tenha selecionado **Registro** na lista suspensa **Estágio**, o script é executado novamente em casos de registro, ativação e reinicialização do dispositivo CPE.
   - Caso tenha selecionado **Exclusão** na lista suspensa **Estágio**, o script não será executado novamente.
   - Caso tenha selecionado **Manualmente** na lista suspensa **Estágio**, o script é executado novamente em casos de ativação e reinicialização do dispositivo CPE.

10. No campo **Script**, insira o caminho do arquivo de script ou do arquivo de script do manual do Ansible.

11. Se necessário, no campo **Arquivo**, especifique o caminho do arquivo comprimido com os arquivos adicionais necessários para executar o script. Formatos compatíveis de arquivos compactados: TAR.GZ e ZIP.

12. Clique em **Salvar**.

    O script é criado e exibido na tabela.

13. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE.

Executar manualmente um script em dispositivos CPE

É possível executar manualmente um único script ou todos os scripts em um modelo de CPE ou em um dispositivo CPE. Os scripts iniciados em um modelo de CPE são executados automaticamente em todos os dispositivos CPE que usam o modelo ou em dispositivos CPE com tags específicas.

Executar manualmente scripts em um modelo de CPE

Para executar manualmente scripts em um modelo de CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE no qual deseja executar scripts manualmente.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Selecione a guia **Scripts**.

   Isso exibirá o número da porta que o VNFM usa para estabelecer a conexão com o dispositivo CPE, o nome de usuário para execução de scripts e a tabela de scripts se pelo menos um script tiver sido adicionado.

4. Para executar manualmente um único script:

   a. Clique em **Executar** ao lado do script que deseja executar manualmente.

   b. Na janela aberta, selecione os dispositivos CPE nos quais deseja executar o script:

   - **Run the script <nome do script> on all related CPEs** executa o script em todos os dispositivos CPE que usam o modelo de CPE. Essa é a configuração padrão.
   - **Run <nome do script> on all related CPEs with specified tags** executa o script em dispositivos CPE que usam o modelo de CPE e têm tags específicas atribuídas. Ao selecionar esse valor, especifique as tags na parte inferior da janela.

5. Para executar manualmente todos os scripts:

   a. Na parte superior da área de configurações, em **Ações**, clique em **Executar scripts**.

   b. Na janela aberta, selecione os dispositivos CPE nos quais deseja executar os scripts:

   - **Executar todos os scripts em CPEs relacionados** para executar os scripts em todos os dispositivos CPE que usam o modelo de CPE. Essa é a configuração padrão.
   - **Executar todos os scripts em CPEs relacionados com as tags especificadas** para executar os scripts em dispositivos CPE que usam o modelo de CPE e têm tags específicas. Ao selecionar esse valor, especifique as tags na parte inferior da janela.

6. Clique em **Executar**.

Os scripts são executados.

Executar scripts manualmente em um dispositivo CPE

Para executar scripts manualmente em um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja executar scripts manualmente.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Scripts**.

   Isso exibirá o número da porta que o VNFM usa para estabelecer a conexão com o dispositivo CPE, o nome de usuário para execução de scripts e a tabela de scripts se pelo menos um script tiver sido adicionado.

4. Execute manualmente os scripts de uma das seguintes formas:

   - Para executar manualmente um único script, clique em **Executar** ao lado do script relevante.
   - Para executar manualmente todos os scripts, na parte superior da área de configurações, em **Ações**, clique em **Executar scripts**.

5. Na janela aberta, clique em **Executar**.

Os scripts são executados.

Agendar scripts em dispositivos CPE

Tarefas agendadas de execução de scripts em dispositivos CPE podem ser criadas no agendador de tarefas. Ao criar uma tarefa, selecione um modelo de CPE, scripts e dispositivos CPE nos quais deseja executar os scripts.

É possível executar scripts em todos os dispositivos CPE que usam um modelo de CPE ou restringir o número de dispositivos CPE especificando tags ou selecionando os dispositivos manualmente.

Para criar uma tarefa para executar scripts em dispositivos CPE:

1. No menu, acesse a seção **Programador**.

   A tabela de tarefas agendadas é exibida.

2. Na parte superior da página, clique em **+ Tarefa**.

3. Na janela aberta, na lista suspensa **Tipo**, selecione **Execução do script**.

4. No campo **Nome**, insira o nome da tarefa.

5. Na lista suspensa **CPEs nos quais executar o script**, selecione os dispositivos CPE nos quais deseja executar o script:

   - **Todos os CPEs com o modelo selecionado** para executar os scripts em todos os dispositivos CPE que usam o modelo de CPE.

   - **Todos os CPEs com o modelo selecionado e tags específicas** para executar os scripts em dispositivos CPE que usam o modelo de CPE e têm tags específicas. Ao selecionar esse valor, especifique as tags do dispositivo CPE no campo **Tags**.

   - **CPEs específicos com o modelo selecionado** para executar os scripts em todos os dispositivos CPE selecionados manualmente que usam o modelo de CPE. Ao selecionar esse valor, selecione os dispositivos CPE em **CPEs**.

6. Em **Modelo de CPE**, selecione o modelo de CPE que contém os scripts que deseja executar.

7. Em **Scripts**, selecione os scripts que deseja executar.

8. No campo **Data de execução da tarefa programada**, insira a data e hora em que deseja executar a tarefa. Por padrão, a data e hora especificadas são a data e hora em que você começou a criar a tarefa.

9. Clique em **Criar**.

Uma tarefa agendada de execução de script é criada e exibida na tabela. O status das tarefas é exibido na coluna **Status**. Se a tarefa de execução de script for concluída com êxito, seu status será alterado para **Concluído**.

Editar um script em dispositivos CPE

É possível editar um script no modelo de CPE. Um script editado no modelo de CPE é editado automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar um script em dispositivos CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE no qual deseja editar um script.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão⩓. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Selecione a guia **Scripts**.

   Isso exibirá o número da porta que o VNFM usa para estabelecer a conexão com o dispositivo CPE, o nome de usuário para execução de scripts e a tabela de scripts se pelo menos um script tiver sido adicionado.

4. Clique em **Editar** ao lado do script que deseja editar.

5. Na janela aberta, se necessário, edite as configurações do script. Para obter uma descrição das configurações, consulte as instruções para adicionar um script em dispositivos CPE.

6. Clique em **Salvar**.

   O script é modificado e atualizado na tabela.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE.

Excluir um script em dispositivos CPE

É possível excluir um script no modelo de CPE. Um script excluído do modelo de CPE é excluído automaticamente de todos os dispositivos CPE que usam o modelo.

Os scripts excluídos não podem ser restaurados.

Para excluir um script em dispositivos CPE:

1. No menu, acesse a subseção **SD-WAN → Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão↙↗. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Selecione a guia **Scripts**.

   Isso exibirá o número da porta que o VNFM usa para estabelecer a conexão com o dispositivo CPE, o nome de usuário para execução de scripts e a tabela de scripts se pelo menos um script tiver sido adicionado.

4. Clique em **Excluir** ao lado do script que deseja excluir.

   O script é excluído e não é mais exibido na tabela.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE.

Gerenciar configurações de DNS em dispositivos CPE

Ativar o DNS em interfaces de rede

Por padrão, os servidores DNS especificados ao criar interfaces de rede ou em regras de encaminhamento condicional de DNS não estão ativos em nenhuma interface. Para que o dispositivo CPE processe as consultas DNS, ative o DNS em determinadas interfaces no modelo de CPE ou no dispositivo CPE.

Para ativar o DNS:

1. Ative o DNS de uma das seguintes formas:

   - Para ativar o DNS em interfaces em um modelo de CPE: no menu, acesse a seção **SD-WAN** → **Modelos de CPE** e clique em um modelo de CPE.

   - Para ativar o DNS em interfaces de um dispositivo CPE: no menu, acesse a seção **SD-WAN** → **CPE** e clique em um dispositivos CPE.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

2. No menu à esquerda, selecione a seção **DNS** e, em seguida, a guia **Interfaces de DNS**.

   A tabela **Ativar/desativar servidor DNS por interface** é exibida.

   As interfaces usadas nas tabelas de roteamento e encaminhamento virtual não estão incluídas nesta tabela. Não há suporte para essas interfaces em dispositivos CPE para o processamento de consultas DNS.

3. Ative o botão de alternância na coluna **Ativado** em interfaces para as quais deseja ativar o processamento de consultas DNS.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

O DNS é ativado em interfaces e o dispositivo CPE usa os servidores DNS especificados ao criar interfaces de rede ou em regras de encaminhamento condicional ao processar consultas DNS.

Gerenciar o encaminhamento condicional de DNS

É possível configurar o encaminhamento condicional de DNS em um dispositivo CPE para direcionar solicitações recebidas para servidores DNS upstream conforme o sufixo de nome especificado na consulta DNS (por exemplo, para bloquear acesso a recursos indesejados ou usar servidores DNS internos para recursos corporativos).

Para usar o encaminhamento condicional de DNS, configure regras de encaminhamento para processar consultas DNS e selecione um servidor DNS dependendo do sufixo especificado na regra.

O encaminhamento condicional de DNS não é compatível com o roteamento e encaminhamento virtual: um dispositivo CPE não pode usar interfaces usadas em uma instância de VRF para processar consultas DNS.

Criar regras de encaminhamento condicional

É possível criar regras de encaminhamento condicional em um modelo de CPE ou em um dispositivo CPE. Regras criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Por padrão, os servidores DNS não estão ativos em nenhuma interface. Para que o dispositivo CPE processe as consultas DNS, ative o DNS em determinadas interfaces.

Para criar uma regra de encaminhamento condicional:

1. Crie um encaminhamento condicional de uma das seguintes formas:

   - Para criar uma regra de encaminhamento condicional em um modelo de CPE: no menu, acesse a seção **SD-WAN** → **Modelos de CPE** e clique em um modelo de CPE.
   - Para criar uma regra de encaminhamento condicional em um dispositivo CPE: no menu, acesse a seção **SD-WAN** → **CPE** e clique em um dispositivo CPE.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

2. No menu à esquerda, selecione a seção **DNS** e, em seguida, a guia **Encaminhamento condicional de DNS**.

   A tabela de regras de encaminhamento condicional é exibida.

3. Na parte superior da tabela, clique em **+ Criar**.

4. Na janela aberta, gerencie as configurações da regra de encaminhamento:

   a. Ative o botão **Ativado** caso deseje que a regra criada seja usada no dispositivo CPE. Deixe o botão desativado para criar uma regra sem aplicá-la ao dispositivo CPE.

   b. No campo **Sufixo**, especifique o sufixo que encaminhará as solicitações de DNS para o servidor DNS com o endereço IP especificado.

   O sufixo de cada regra deve ser único. O comprimento máximo é de 255 caracteres. O valor do campo deve ser uma string no seguinte formato:

   ```
   <label1>[.<label>]
   ```

   (o item `<label1>` seguido pelo conjunto opcional de itens `<label>` separados por pontos), em que `<label>` é uma substring composta de caracteres `[a-zA-Z0-9-]` com comprimento de 1 a 63 caracteres, `<label1>` é uma substring composta dos mesmos caracteres permitidos com um caractere curinga * opcional no início.

   Se o sufixo incluir um ou mais `<label>` após `<label1>`, `<label1>` poderá conter apenas o caractere *; se o sufixo não tiver nenhum item `<label>`, `<label1>` deve ter outros caracteres permitidos após *.

   Exemplos:

   Valores possíveis:

   *.exemplo.com

   *exemplo.com

   Valores inválidos:

   *

www.*.com

www.*exemplo.com

c. Adicione um ou mais servidores DNS upstream para os quais deseja encaminhar consultas DNS:

- No campo **DNS upstream**, insira o endereço IP do servidor DNS para o qual deseja encaminhar consultas DNS quando o sufixo dessa regra for correspondente.
- Na lista **Alias**, selecione o alias da interface a partir da qual deseja enviar consultas DNS para essa regra.

Se necessário, clique no botão **Adicionar DNS upstream** para adicionar o próximo servidor DNS upstream. É possível adicionar até 15 servidores DNS upstream para cada sufixo.

5. Clique em **Salvar**.

   A regra de encaminhamento condicional é criada e exibida na tabela.

6.

7. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar regras de encaminhamento condicional

É possível editar regras de encaminhamento condicional em um modelo de CPE ou em um dispositivo CPE. As regras editadas no modelo de CPE são automaticamente editadas em todos os dispositivos CPE que usam o modelo.

Para editar uma regra de encaminhamento condicional:

1. Edite um encaminhamento condicional de uma das seguintes formas:

   - Para editar uma regra de encaminhamento condicional em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu e clique no modelo de CPE no qual deseja editar a regra de encaminhamento condicional.
   - Para editar uma regra de encaminhamento condicional em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu e clique no dispositivo CPE no qual deseja editar a regra de encaminhamento condicional.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

2. No menu à esquerda, selecione a seção **DNS** e, em seguida, a guia **Encaminhamento condicional de DNS**.

   A tabela de regras de encaminhamento condicional é exibida.

3. Selecione a regra de encaminhamento condicional que deseja editar e clique no botão **Editar**.

4. Na janela aberta, edite as configurações da regra de encaminhamento conforme necessário. Para obter uma descrição das configurações, consulte o artigo Criar regras de encaminhamento condicional.

5. Clique em **Salvar**.

   A regra de encaminhamento condicional é modificada e atualizada na tabela.

6. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir regras de encaminhamento condicional

Para excluir regras de encaminhamento condicional:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja excluir regras.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. No menu à esquerda, selecione a seção **DNS** e, em seguida, a guia **Encaminhamento condicional de DNS**.

   A tabela de regras de encaminhamento condicional é exibida.

4. Selecione uma ou mais regras de encaminhamento condicional que deseja excluir e clique no botão **Excluir**.

5. Na janela de confirmação, clique em **Excluir**.

As regras de encaminhamento condicional são excluídas e não são mais exibidas na tabela.

Configurar a conexão de um dispositivo CPE com orquestrador e controlador

Quando um dispositivo CPE está sendo registrado, ele faz a conexão com o orquestrador e o controlador. É possível especificar as configurações de conexão do orquestrador e do controlador em um modelo de CPE ou em um dispositivo CPE. As configurações de conexão do orquestrador e do controlador especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Alguns modelos de CPE de hardware têm LEDs adicionais que exibem o status da conexão do controlador, a conexão do orquestrador e se há túneis ativos caso a função CPE esteja ativada. Para obter mais informações sobre os LEDs, consulte a documentação dos dispositivos ou entre em contato com o Suporte Técnico.

Para configurar a conexão de um dispositivo CPE com orquestrador e controlador:

1. Configure a conexão do orquestrador e do controlador do dispositivo CPE de uma das seguintes formas:

   - Para configurar a conexão automática com orquestrador e controlador em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **SD-WAN → Configurações gerais**.

   - Para configurar a conexão automática com orquestrador e controlador em um modelo de CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **SD-WAN → Configurações gerais** e marque a caixa de seleção **Substituir**.

   Isso exibe as configurações de conexão de um dispositivo CPE com orquestrador e controlador.

2. Em **Conexão com o orquestrador**, especifique as configurações de conexão do orquestrador do dispositivo CPE:

   a. No campo **Endereço IP/FQDN do orquestrador**, insira o endereço IP ou FQDN do orquestrador. O comprimento máximo do FQDN é de 50 caracteres.

   b. No campo **Porta do orquestrador**, insira o número da porta do orquestrador. Intervalo de valores: 0 a 65.535.

   c. Caso deseje que o dispositivo CPE obtenha o número da porta do orquestrador via DNS, ative o botão **Obter porta do orquestrador via DNS**. Para usar essa função, primeiro crie um registro TXT no servidor DNS que armazene o número da porta necessária no formato `_port.<FQDN>`, em que `<FQDN>` é o endereço do orquestrador especificado no campo **Endereço IP/FQDN do orquestrador**.

   d. Para usar um orquestrador de backup caso o orquestrador principal falhe, em **Endereço IP e porta do orquestrador de backup**:

      1. Marque a caixa de seleção **Ativado**. Esta caixa de seleção está desmarcada por padrão.

      2. No campo **Endereço IP/FQDN do orquestrador de backup**, insira o endereço IP ou FQDN do orquestrador de backup. O comprimento máximo do FQDN é de 50 caracteres.

      3. No campo **Porta do orquestrador de backup**, insira o número da porta do orquestrador de backup. Intervalo de valores: 0 a 65.535.

   e. Na lista suspensa **Protocolo do orquestrador**, selecione o protocolo para conectar o dispositivo CPE ao orquestrador:

      - **http**.

      - **https**. Essa é a configuração padrão.

      Essa configuração só pode ser especificada em um modelo de CPE.

   f. No campo **Intervalo de atualização (s)**, insira o período em segundos para enviar solicitações de API REST do dispositivo CPE para o orquestrador. Intervalo de valores: 5 a 300. O valor padrão é `30`.

g. No campo **Intervalo de atualização interativa (s)**, insira o período em segundos para enviar solicitações de API REST do dispositivo CPE para o orquestrador no modo interativo. Intervalo de valores: 1 a 10. É possível ativar o modo interativo para o diagnóstico do dispositivo CPE.

h. No campo **Tempo limite do modo interativo (s)**, insira o tempo em segundos após o qual o modo interativo é automaticamente desativado no dispositivo CPE. Intervalo de valores: 30 a 180.

3. Em **Conexão com o controlador**, especifique as configurações de conexão do controlador do dispositivo CPE:

a. Na lista suspensa **Transporte OpenFlow**, especifique se as sessões de gerenciamento entre as interfaces SD-WAN do tipo WAN do dispositivo CPE e os nós do controlador são criptografadas:

- **TCP** para sessões de gerenciamento não criptografadas.
- **SSL** para sessões de gerenciamento criptografadas. Essa é a configuração padrão.

Essa configuração só pode ser especificada em um modelo de CPE.

b. Na lista suspensa **Interface do plano de controle priorizado**, selecione a interface SD-WAN do tipo WAN que tem prioridade ao estabelecer a sessão de gerenciamento principal:

- **Aleatório** significa que a sessão de gerenciamento principal é estabelecida a partir de uma interface SD-WAN do tipo WAN escolhida aleatoriamente. Essa é a configuração padrão.
- **<Interface SD-WAN do tipo WAN>** significa que a interface SD-WAN do tipo WAN especificada é usada para estabelecer a sessão de gerenciamento principal. Se a interface SD-WAN do tipo WAN especificada não estiver disponível, a sessão de gerenciamento principal é estabelecida a partir de uma interface SD-WAN do tipo WAN escolhida aleatoriamente.

Se a interface SD-WAN do tipo WAN da qual a sessão de gerenciamento principal foi estabelecida falhar, uma nova sessão de gerenciamento principal será selecionada aleatoriamente a partir das sessões de gerenciamento estabelecidas anteriormente. Caso tenha selecionado **<interface SD-WAN do tipo WAN>** na lista suspensa **Interface do plano de controle priorizado** e desejar que a sessão de gerenciamento estabelecida a partir da interface SD-WAN do tipo WAN especificada se torne a sessão principal novamente quando a interface for recuperada:

1. Selecione a caixa de seleção **Preemptividade**. Esta caixa de seleção está desmarcada por padrão.
2. No campo **Tempo esgotado**, insira o tempo em segundos após o qual a sessão de gerenciamento estabelecida a partir da interface SD-WAN do tipo WAN especificada se torna a principal novamente quando a interface for recuperada. Intervalo de valores: 0 a 86.400.

c. Na lista suspensa **Reinicialização automática**, selecione se deseja que o dispositivo CPE reinicie quando as sessões de gerenciamento com nós do controlador forem interrompidas por um longo período:

- **Sim**. Ao selecionar essa opção, no campo **Tempo limite de reinicialização (s)**, insira o tempo em segundos após o qual o dispositivo CPE é reiniciado automaticamente quando as sessões de gerenciamento com nós do controlador são interrompidas. Intervalo de valores: 60 a 2.073.600.
- **Não**. Essa é a configuração padrão.

d. No campo **URL de configuração**, insira o modelo de URL para as configurações básicas do dispositivo CPE. Ao inserir um modelo, considere as seguintes limitações:

- `{config}` é uma parte obrigatória que é substituída pelas configurações do dispositivo CPE quando um link é gerado a partir do modelo.
- Comprimento máximo: 128 caracteres.
- Especifique `http` ou `https`.

Por padrão, o seguinte modelo de URL é usado: `http://192.168.7.1/cgi-bin/config?payload={config}`.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar as configurações de conexão do dispositivo CPE usando o console do sistema

É possível abrir uma sessão do console em um dispositivo CPE para restaurar o firmware ou realizar diagnósticos. Os modelos M2 e posteriores são equipados com uma porta serial externa para conexão com o console do sistema. Para o modelo M1, é possível estabelecer uma conexão com o console do sistema através do conector UART, localizado sob a tampa do dispositivo, usando um adaptador.

Após obter acesso ao console do sistema, forneça suas credenciais de login. Configure a autenticação no console do sistema usando a interface da Web do orquestrador em um modelo de CPE ou no dispositivo CPE.

Para configurar a autenticação no console do sistema:

1. Configure a autenticação no console do sistema usando um dos seguintes métodos:

- Para configurar a autenticação no console do sistema em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **SD-WAN → Configurações gerais**.
- Para configurar a conexão com o console do sistema em um modelo de CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **SD-WAN → Configurações gerais** e marque a caixa de seleção **Substituir**.

As configurações de conexão do dispositivo CPE são exibidas.

2. Em **Configurações do console**, ative o botão **Autenticação no console do sistema** para solicitar credenciais do usuário ao estabelecer a conexão por meio do console do sistema, ou desative o botão para desativar a solicitação de credenciais. Esse botão é desativado por padrão.

3. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Para que a alteração tenha efeito, reinicie o dispositivo manualmente.

Gerenciar interfaces de rede

As *interfaces de rede* correspondem às portas e interfaces virtuais do sistema operacional do dispositivo CPE que estabelecem conexão com a WAN ou LAN. É necessário mapear as interfaces de rede do dispositivo CPE para as portas OpenFlow do switch virtual usando interfaces SD-WAN.

Para visualizar a tabela de interfaces de rede em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de interfaces de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Rede**.
- Para visualizar a tabela de interfaces de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Rede**.

As informações sobre as interfaces de rede são exibidas nas seguintes colunas da tabela:

- **Substituir**:
  - **Sim** significa que as configurações da interface de rede não são herdadas de um modelo.
  - **Não** significa que as configurações da interface de rede são herdadas de um modelo.

  Essa coluna é exibida apenas no dispositivo CPE. É possível alterar o valor nessa coluna para cada interface de rede diretamente na tabela.
- **Ativado**:
  - **Sim** significa que a interface de rede está ativada.
  - **Não** significa que a interface de rede está desativada.

  É possível alterar o valor nessa coluna para cada interface de rede diretamente na tabela no dispositivo CPE após selecionar **Sim** na coluna **Substituir**.
- **Herdado** indica se a interface de rede é herdada de um modelo de CPE:
  - **Sim**.
  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.
- **Alias** é o alias da interface de rede para mapeá-la para uma porta OpenFlow. É necessário especificar esse alias de interface de rede ao criar uma interface SD-WAN do tipo WAN.
- **Descrição** é uma breve descrição da interface de rede.
- **Zona**é a zona do firewall.
- **Índice de interface NetFlow** é a ID numérica permanente da interface usada ao enviar estatísticas através do protocolo NetFlow.

  Essa coluna está oculta por padrão.

- **Nome da interface** é o nome da porta física ou interface virtual do sistema operacional do dispositivo CPE.
- **Protocolo** é o método de atribuição de um endereço IP à interface de rede:
  - **Cliente DHCP** significa que o endereço IP é atribuído automaticamente pelo DHCP.
  - **Endereço IPv4 estático** significa que um endereço IPv4 é atribuído estaticamente.
  - **Endereço IPv6 estático** significa que um endereço IPv6 é atribuído estaticamente.
  - **QMI** significa que as configurações de conexão de rede LTE são especificadas manualmente.
  - **PPPoE** significa que as configurações de conexão do servidor PPPoE são especificadas manualmente.
  - **Nenhum** significa que não há um endereço IP atribuído.
- **Endereço/máscara IP** são o endereço IP, a máscara e o gateway padrão da interface de rede.
- **MTU** é o valor de MTU para a interface de rede.
- **Ativa automaticamente** indica se a interface de rede é ativada automaticamente quando o dispositivo CPE é ligado:
  - **Sim**.
  - **Não**.

As ações que podem ser executadas com as tabelas são descritas nas instruções Gerenciar tabelas de componentes da solução.

Criar interfaces de rede

É possível criar uma interface de rede em um modelo de CPE ou dispositivo CPE. Interfaces de rede criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Criar uma interface de rede com atribuição automática de um endereço IP via DHCP

Para criar uma interface de rede com atribuição automática de um endereço IP via DHCP:

1. Crie uma interface de rede de uma das seguintes formas:
   - Para criar uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE**, clique no modelo de CPE e selecione a guia **Rede**.
   - Para criar uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Rede**.

   A tabela de interfaces de rede é exibida.
2. Clique em **+ Interface de rede**.

3. Na janela aberta, no campo **Alias**, insira o nome da interface de rede para mapeá-la para uma porta OpenFlow. É necessário especificar esse nome de interface de rede ao criar uma interface SD-WAN do tipo WAN. O comprimento máximo do nome é de 15 caracteres.

4. Para adicionar uma interface de rede a uma zona de firewall, na lista suspensa **Zona**, selecione a zona de firewall criada.

5. No campo **Nome da interface**, insira o nome da porta física ou interface virtual do sistema operacional do dispositivo CPE. O comprimento máximo do nome é de 256 caracteres. Por exemplo, é possível inserir `eth0`, `eth1`, `eth2` ou `tun0`. Para criar uma ponte de várias interfaces, insira os nomes delas separados por espaços.

   Para atribuir uma tag de VLAN externa a uma interface de rede, insira um ponto (.) após o nome da porta física ou interface virtual do sistema operacional e, em seguida, insira a tag de VLAN externa. Por exemplo, `eth2.150`.

6. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535. Para criar uma ponte a partir de interfaces físicas ou virtuais cujos nomes estão especificados no campo **Nome da interface**:

   a. Marque a caixa de seleção **Ponte**. Esta caixa de seleção está desmarcada por padrão.

   b. Para usar o STP na ponte para evitar loops de roteamento, selecione a caixa de seleção **STP**. Esta caixa de seleção está desmarcada por padrão.

   c. No campo **Idade (s)**, insira o tempo, em segundos, durante o qual os registros dinâmicos são armazenados na tabela MAC da ponte. Para usar a ponte como um hub, insira `0` nesse campo. Intervalo de valores: 0 a 86.400.

7. Para ativar o protocolo NetFlow na interface de rede, marque a caixa de seleção **NetFlow**. Esta caixa de seleção está desmarcada por padrão.

8. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535.

9. Na lista suspensa **Protocolo**, selecione **Cliente DHCP**.

10. Caso não queira que a interface de rede seja ativada automaticamente quando o dispositivo CPE for ativado, desmarque a caixa de seleção **Ativa automaticamente**. Esta caixa de seleção é selecionada por padrão.

11. Para que um endereço IP, uma rota e um gateway padrão sejam atribuídos automaticamente à interface de rede, marque a caixa de seleção **Forçar endereço IP, rota e gateway**. Esta caixa de seleção está desmarcada por padrão.

12. Caso não queira que a rota obtida via DHCP seja usada pela interface de rede por padrão, desmarque a caixa de seleção **Usar rota padrão**. Esta caixa de seleção é selecionada por padrão.

13. Se necessário, especifique um servidor DNS para a interface de rede:

    a. Em **Servidores DNS**, clique em **+ Adicionar**.

    b. No campo exibido, insira o endereço IP do servidor DNS.

    O servidor DNS é especificado e exibido na seção **Servidores DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique no ícone de exclusão ✕ ao lado dele.

14. No campo **Substituir MAC**, insira o endereço MAC da interface de rede. O valor inserido substitui o endereço MAC real da interface de rede. O campo não pode ser editado se a caixa de seleção **Gerar endereço MAC automaticamente** estiver marcada.

15. No campo **Substituir MTU**, insira a MTU para a interface de rede. O valor inserido substitui a MTU padrão.

16. Para que o endereço MAC da interface de rede seja gerado automaticamente, marque a caixa de seleção **Gerar endereço MAC automaticamente** (desmarcada por padrão).

17. Se necessário, no campo **Métrica de roteamento**, insira a métrica de roteamento padrão para a interface de rede. O dispositivo CPE usa o roteamento padrão com a métrica mais baixa.

    A métrica de roteamento para interfaces de rede com aliases **sdwan0**–**sdwan3** é atribuída automaticamente na inicialização do CPE: a **sdwan0** obtém a prioridade mais alta e a prioridade mais baixa vai para **sdwan3.** Nesse caso, o dispositivo CPE usa o roteamento padrão da interface de rede **sdwan0**. Se a interface de rede **sdwan0** falhar, o roteamento padrão da interface de rede **sdwan1** é então usado, seguido pela rota padrão da interface de rede **sdwan2**. O valor no campo **Métrica de roteamento** está bloqueado para edição manual para interfaces com os aliases **sdwan0**–**sdwan9**.

    A métrica é calculada automaticamente a partir dos seguintes atributos:

    - `1–4` se não houver erros e houver acesso à Internet
    - `11–14` se não houver erros e não houver acesso à Internet
    - `21–24` se houver erros e não houver acesso à Internet.

    As métricas são atribuídas automaticamente às interfaces dependendo do número final da alias da interface, de acordo com o seguinte esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

18. Clique em **Criar**.

    A interface de rede é criada e exibida na tabela.

19. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Criar uma interface de rede com um endereço IPv4 estático

Para criar uma interface de rede com um endereço IPv4 estático:

1. Crie uma interface de rede de uma das seguintes formas:

    - Para criar uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE**, clique no modelo de CPE e selecione a guia **Rede**.
    - Para criar uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Rede**.

    A tabela de interfaces de rede é exibida.

2. Clique em **+ Interface de rede**.

3. Na janela aberta, no campo **Alias**, insira o nome da interface de rede para mapeá-la para uma porta OpenFlow. É necessário especificar esse nome de interface de rede ao criar uma interface SD-WAN do tipo WAN. O comprimento máximo do nome é de 15 caracteres.

4. Para adicionar uma interface de rede a uma zona de firewall, na lista suspensa **Zona**, selecione a zona de firewall criada.

5. No campo **Nome da interface**, insira o nome da porta física ou interface virtual do sistema operacional do dispositivo CPE. O comprimento máximo do nome é de 256 caracteres. Por exemplo, é possível inserir `eth0`, `eth1`, `eth2` ou `tun0`. Para criar uma ponte de várias interfaces, insira os nomes delas separados por espaços.

   Para atribuir uma tag de VLAN externa a uma interface de rede, insira um ponto (.) após o nome da porta física ou interface virtual do sistema operacional e, em seguida, insira a tag de VLAN externa. Por exemplo, `eth2.150`.

6. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535. Para criar uma ponte a partir de interfaces físicas ou virtuais cujos nomes estão especificados no campo **Nome da interface**:

   a. Marque a caixa de seleção **Ponte**. Esta caixa de seleção está desmarcada por padrão.

   b. Para usar o STP na ponte para evitar loops de roteamento, selecione a caixa de seleção **STP**. Esta caixa de seleção está desmarcada por padrão.

   c. No campo **Idade (s)**, insira o tempo, em segundos, durante o qual os registros dinâmicos são armazenados na tabela MAC da ponte. Para usar a ponte como um hub, insira `0` nesse campo. Intervalo de valores: 0 a 86.400.

7. Para ativar o protocolo NetFlow na interface de rede, marque a caixa de seleção **NetFlow**. Esta caixa de seleção está desmarcada por padrão.

8. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535.

9. Na lista suspensa **Protocolo**, selecione **Endereço IPv4 estático**.

10. Caso não queira que a interface de rede seja ativada automaticamente quando o dispositivo CPE for ativado, desmarque a caixa de seleção **Ativa automaticamente**. Esta caixa de seleção é selecionada por padrão.

11. Para que um endereço IP, uma rota e um gateway padrão sejam atribuídos automaticamente à interface de rede, marque a caixa de seleção **Forçar endereço IP, rota e gateway**. Esta caixa de seleção está desmarcada por padrão.

12. Na lista suspensa **Tipo de entrada de endereço IPv4 e máscara de sub-rede**, selecione o método para a atribuição de um endereço IPv4 à interface de rede:

    - **Manualmente** para atribuir um endereço IPv4 manualmente. Ao selecionar essa opção, faça o seguinte:

      a. No campo **Endereço IPv4**, insira o endereço IPv4 da interface de rede.

      b. No campo **Netmask IPv4**, insira a máscara de sub-rede da interface de rede.

    Essa é a configuração padrão.

- **Do pool de IP** para atribuir um endereço IPv4 do intervalo de endereços IP especificado. Ao selecionar esse valor, na lista suspensa **Pool de endereço IP**, selecione um intervalo de endereços IP criado.

- **Do pool de sub-rede** para atribuir um endereço IPv4 do intervalo de sub-redes especificado. Ao selecionar esse valor, na lista suspensa **Pool de sub-rede**, selecione um intervalo de sub-redes criado.

13. No campo **Gateway IPv4**, insira o endereço IPv4 do gateway padrão.

14. No campo **Difusão IPv4**, insira o endereço de difusão da interface de rede. Caso não seja especificado um valor para essa configuração, ela será gerada automaticamente.

15. Se necessário, especifique um servidor DNS para a interface de rede:

    a. Em **Servidores DNS**, clique em **+ Adicionar**.

    b. No campo exibido, insira o endereço IP do servidor DNS.

    O servidor DNS é especificado e exibido na seção **Servidores DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique no ícone de exclusão ✕ ao lado dele.

16. No campo **Substituir MAC**, insira o endereço MAC da interface de rede. O valor inserido substitui o endereço MAC real da interface de rede.

17. No campo **Substituir MTU**, insira a MTU para a interface de rede. O valor inserido substitui a MTU padrão.

18. Se necessário, no campo **Métrica de roteamento**, insira a métrica de roteamento padrão para a interface de rede. O dispositivo CPE usa o roteamento padrão com a métrica mais baixa.

    A métrica de roteamento para interfaces de rede com aliases **sdwan0**–**sdwan3** é atribuída automaticamente na inicialização do CPE: a **sdwan0** obtém a prioridade mais alta e a prioridade mais baixa vai para **sdwan3.** Nesse caso, o dispositivo CPE usa o roteamento padrão da interface de rede **sdwan0**. Se a interface de rede **sdwan0** falhar, o roteamento padrão da interface de rede **sdwan1** é então usado, seguido pela rota padrão da interface de rede **sdwan2**. O valor no campo **Métrica de roteamento** está bloqueado para edição manual para interfaces com os aliases **sdwan0**–**sdwan9**.

    A métrica é calculada automaticamente a partir dos seguintes atributos:

    - `1–4` se não houver erros e houver acesso à Internet
    - `11–14` se não houver erros e não houver acesso à Internet
    - `21–24` se houver erros e não houver acesso à Internet.

    As métricas são atribuídas automaticamente às interfaces dependendo do número final da alias da interface, de acordo com o seguinte esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

19. Em **Servidor DHCP**, na lista suspensa **Tipo**, selecione o modo de operação do servidor DHCP para a interface de rede:

    - **Desativado**. Essa é a configuração padrão.
    - **Relé** Ao selecionar esse valor, insira o endereço IP do servidor DHCP no campo **IP do servidor DHCP**.
    - **Servidor**

20. Caso tenha selecionado **Servidor** na lista suspensa **Tipo**, especifique as configurações do servidor DHCP:

    a. No campo **Primeiro IP**, insira o deslocamento do endereço IP base da interface de rede para derivar o endereço IP mais baixo que pode ser concedido aos clientes. O valor padrão é `100`. É possível inserir um valor maior que 255 para sub-redes grandes.

    b. No campo **Limite**, insira o número máximo de endereços IP que podem ser concedidos aos clientes. Intervalo de valores: 1 a 250. O valor padrão é `150`.

    c. No campo **Tempo de concessão**, insira o tempo máximo, em horas, que um endereço IP individual pode ser concedido a um cliente. Intervalo de valores: 1 a 250. O valor é especificado no seguinte formato: `< número de horas >h`. Por exemplo, para que o tempo máximo de concessão seja de 5 horas, insira `5h`. O valor padrão é `12h`.

    d. Se necessário, especifique uma opção de DHCP:

        1. Em **Opções do DHCP**, clique em **+ Adicionar**.
        2. No campo exibido, insira o número da opção de DHCP de acordo com o padrão RFC 1533. Comprimento máximo: 250 caracteres.

        A opção de DHCP é especificada e exibida em **Opções do DHCP**. É possível especificar várias opções de DHCP ou excluir opções de DHCP. Para excluir uma opção de DHCP, clique no ícone de exclusão ✕ ao lado dela.

21. Clique em **Criar**.

    A interface de rede é criada e exibida na tabela.

22. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Criar uma interface de rede com um endereço IPv6 estático

Para criar uma interface de rede com um endereço IPv6 estático:

1. Crie uma interface de rede de uma das seguintes formas:

    - Para criar uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE**, clique no modelo de CPE e selecione a guia **Rede**.
    - Para criar uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Rede**.

    A tabela de interfaces de rede é exibida.

2. Clique em **+ Interface de rede**.

3. Na janela aberta, no campo **Alias**, insira o nome da interface de rede para mapeá-la para uma porta OpenFlow. É necessário especificar esse nome de interface de rede ao criar uma interface SD-WAN do tipo WAN. O comprimento máximo do nome é de 15 caracteres.

4. Para adicionar uma interface de rede a uma zona de firewall, na lista suspensa **Zona**, selecione a zona de firewall criada.

5. No campo **Nome da interface**, insira o nome da porta física ou interface virtual do sistema operacional do dispositivo CPE. O comprimento máximo do nome é de 256 caracteres. Por exemplo, é possível inserir `eth0`, `eth1`, `eth2` ou `tun0`. Para criar uma ponte de várias interfaces, insira os nomes delas separados por espaços.

   Para atribuir uma tag de VLAN externa a uma interface de rede, insira um ponto (.) após o nome da porta física ou interface virtual do sistema operacional e, em seguida, insira a tag de VLAN externa. Por exemplo, `eth2.150`.

6. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535. Para criar uma ponte a partir de interfaces físicas ou virtuais cujos nomes estão especificados no campo **Nome da interface**:

   a. Marque a caixa de seleção **Ponte**. Esta caixa de seleção está desmarcada por padrão.

   b. Para usar o STP na ponte para evitar loops de roteamento, selecione a caixa de seleção **STP**. Esta caixa de seleção está desmarcada por padrão.

   c. No campo **Idade (s)**, insira o tempo, em segundos, durante o qual os registros dinâmicos são armazenados na tabela MAC da ponte. Para usar a ponte como um hub, insira `0` nesse campo. Intervalo de valores: 0 a 86.400.

7. Para ativar o protocolo NetFlow na interface de rede, marque a caixa de seleção **NetFlow**. Esta caixa de seleção está desmarcada por padrão.

8. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535.

9. Na lista suspensa **Protocolo**, selecione **Endereço IPv6 estático**.

10. Caso não queira que a interface de rede seja ativada automaticamente quando o dispositivo CPE for ativado, desmarque a caixa de seleção **Ativa automaticamente**. Esta caixa de seleção é selecionada por padrão.

11. Para que um endereço IP, uma rota e um gateway padrão sejam atribuídos automaticamente à interface de rede, marque a caixa de seleção **Forçar endereço IP, rota e gateway**. Esta caixa de seleção está desmarcada por padrão.

12. No campo **Endereço IPv6**, insira o endereço IPv6 da interface de rede. É possível especificar vários endereços separando-os com espaços.

13. No campo **Sufixo IPv6**, insira o sufixo IPv6 da interface de rede. Comprimento máximo: 30 caracteres.

14. No campo **Gateway IPv6**, insira o endereço IPv6 do gateway padrão.

15. No campo **Comprimento do prefixo**, insira o comprimento do prefixo IPv6 da interface de rede. Intervalo de valores: 12 a 127.

16. No campo **Comprimento do subprefixo DHCPv6**, insira o tamanho do subprefixo DHCPv6 da interface de rede. Comprimento máximo: 256 caracteres.

17. No campo **Prefixo IPv6**, insira o prefixo IPv6 da interface de rede. Comprimento máximo: 30 caracteres.

18. Caso deseje que a interface de rede aceite a classe de prefixo IPv6 especificada, faça o seguinte:

    a. Em **Classe IPv6**, clique em **+ Adicionar**.

    b. Insira o nome da classe de prefixo IPv6 no campo exibido. Comprimento máximo: 256 caracteres.

    A classe de prefixo IPv6 é especificada e exibida em **Classe IPv6**. É possível especificar várias classes de prefixo IPv6 ou excluir classes de prefixo IPv6. Para excluir uma classe de prefixo IPv6, clique no ícone de exclusão ✕ ao lado dela.

19. Se necessário, especifique um servidor DNS para a interface de rede:

    a. Em **Servidores DNS**, clique em **+ Adicionar**.

    b. No campo exibido, insira o endereço IP do servidor DNS.

    O servidor DNS é especificado e exibido na seção **Servidores DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique no ícone de exclusão ✕ ao lado dele.

20. No campo **Substituir MAC**, insira o endereço MAC da interface de rede. O valor inserido substitui o endereço MAC real da interface de rede.

21. No campo **Substituir MTU**, insira a MTU para a interface de rede. O valor inserido substitui a MTU padrão.

22. Se necessário, no campo **Métrica de roteamento**, insira a métrica de roteamento padrão para a interface de rede. O dispositivo CPE usa o roteamento padrão com a métrica mais baixa.

    A métrica de roteamento para interfaces de rede com aliases **sdwan0**–**sdwan3** é atribuída automaticamente na inicialização do CPE: a **sdwan0** obtém a prioridade mais alta e a prioridade mais baixa vai para **sdwan3.** Nesse caso, o dispositivo CPE usa o roteamento padrão da interface de rede **sdwan0**. Se a interface de rede **sdwan0** falhar, o roteamento padrão da interface de rede **sdwan1** é então usado, seguido pela rota padrão da interface de rede **sdwan2**. O valor no campo **Métrica de roteamento** está bloqueado para edição manual para interfaces com os aliases **sdwan0**–**sdwan9**.

    A métrica é calculada automaticamente a partir dos seguintes atributos:

    - `1–4` se não houver erros e houver acesso à Internet
    - `11–14` se não houver erros e não houver acesso à Internet
    - `21–24` se houver erros e não houver acesso à Internet.

    As métricas são atribuídas automaticamente às interfaces dependendo do número final da alias da interface, de acordo com o seguinte esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

23. Em **Servidor DHCP**, na lista suspensa **Tipo**, selecione o modo de operação do servidor DHCP para a interface de rede:

    - **Desativado**. Essa é a configuração padrão.
    - **Relé** Ao selecionar esse valor, insira o endereço IP do servidor DHCP no campo **IP do servidor DHCP**.
    - **Servidor**

24. Caso tenha selecionado **Servidor** na lista suspensa **Tipo**, especifique as configurações do servidor DHCP:

    a. No campo **Primeiro IP**, insira o deslocamento do endereço IP base da interface de rede para derivar o endereço IP mais baixo que pode ser concedido aos clientes. O valor padrão é `100`. É possível inserir um valor maior que 255 para sub-redes grandes.

    b. No campo **Limite**, insira o número máximo de endereços IP que podem ser concedidos aos clientes. Intervalo de valores: 1 a 250. O valor padrão é `150`.

    c. No campo **Tempo de concessão**, insira o tempo máximo, em horas, que um endereço IP individual pode ser concedido a um cliente. Intervalo de valores: 1 a 250. O valor é especificado no seguinte formato: `<número de horas>h`. Por exemplo, para que o tempo máximo de concessão seja de 5 horas, insira `5h`. O valor padrão é `12h`.

    d. Se necessário, especifique uma opção de DHCP:

        1. Em **Opções do DHCP**, clique em **+ Adicionar**.
        2. No campo exibido, insira o número da opção de DHCP de acordo com o padrão RFC 1533. Comprimento máximo: 250 caracteres.

        A opção de DHCP é especificada e exibida em **Opções do DHCP**. É possível especificar várias opções de DHCP ou excluir opções de DHCP. Para excluir uma opção de DHCP, clique no ícone de exclusão ✕ ao lado dela.

25. Clique em **Criar**.

    A interface de rede é criada e exibida na tabela.

26. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Criar uma interface de rede para estabelecer conexão com uma rede LTE

Esta funcionalidade não é compatível com alguns modelos. Entre em contato com o Suporte Técnico da Kaspersky.

Para criar uma interface de rede para estabelecer conexão com uma rede LTE:

1. Crie uma interface de rede de uma das seguintes formas:

   - Para criar uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE**, clique no modelo de CPE e selecione a guia **Rede**.
   - Para criar uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Rede**.

   A tabela de interfaces de rede é exibida.

2. Clique em **+ Interface de rede**.
3. Na janela aberta, no campo **Alias**, insira o alias da interface de rede para mapeá-la para uma porta OpenFlow. É necessário especificar esse alias de interface de rede ao criar uma interface SD-WAN do tipo WAN. O comprimento máximo do alias é de 15 caracteres.
4. Para adicionar uma interface de rede a uma zona de firewall, na lista suspensa **Zona**, selecione a zona de firewall criada.
5. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535.
6. Na lista suspensa **Protocolo**, selecione **QMI**.
7. No campo **Nome QMI**, insira o caminho para o modem no dispositivo CPE. O comprimento máximo do caminho é de 30 caracteres. Por exemplo, `/dev/cdc-wdm0`.
8. Na lista **Origem do APN**, selecione como deseja inserir o ID do APN da operadora de telecomunicações que emitiu o cartão SIM instalado no modem:

   - Caso deseje que o APN seja inserido automaticamente a partir do diretório APN, selecione**Diretório** e, em seguida, selecione um diretório na lista **Diretório APN**
   - Para especificar a string APN manualmente, selecione **Manual** e, em seguida, insira a string APN no campo **String do APN** exibido. O comprimento máximo do ID é de 30 caracteres.

9. Na lista suspensa **Tipo de autenticação**, selecione o tipo de autenticação na interface de rede:

   - **PAP** (Protocolo de Autenticação de Senha).
   - **CHAP** (Protocolo de Autenticação por Desafio Handshake).
   - **PAP e CHAP** significa que ambos os tipos de autenticação são usados na interface de rede.
   - **Nenhum** significa que não é usada autenticação na interface de rede.

10. No campo **Nome de usuário para autenticação PAP/CHAP**, insira o nome de usuário para autenticação PAP/CHAP. O comprimento máximo do nome é de 30 caracteres. Caso não queira usar autenticação, não especifique um valor para a configuração.

11. No campo **Senha para autenticação PAP/CHAP**, insira a senha para a autenticação PAP/CHAP. O comprimento máximo da senha é de 30 caracteres. Caso não queira usar autenticação, não especifique um valor para a configuração.

12. No campo **Código PIN**, insira o código PIN do cartão SIM instalado no modem. Comprimento máximo do PIN: 4 dígitos.

13. No campo **Atraso**, insira o tempo, em segundos, após o qual a interface de rede começa a se comunicar com o modem. Valor máximo: 30. Essa configuração é usada quando o modem demora muito para iniciar.

14. Se necessário, especifique os modos de comunicação móvel em que deseja que o modem opere:

    a. Em **Modos**, clique em **+ Adicionar**.

    b. Na lista suspensa, selecione um dos seguintes valores:

    - **Todos**, para usar todos os modos de comunicação móvel disponíveis
    - **LTE**
    - **UMTS**
    - **GSM**
    - **CDMA**
    - **TD-SCDMA**

    Os modos de comunicação móvel são configurados no modem e exibidos em **Modos**. É possível especificar diversos modos ou excluir modos. Para excluir um modo, clique no ícone de exclusão ✕ ao lado dele.

15. Se necessário, especifique um servidor DNS para a interface de rede:

    a. Em **Servidores DNS**, clique em **+ Adicionar**.

    b. No campo exibido, insira o endereço IP do servidor DNS.

    O servidor DNS é especificado e exibido na seção **Servidores DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique no ícone de exclusão ✕ ao lado dele.

16. No campo **Perfil da conexão**, insira o índice do perfil de conexão que a interface de rede usa em vez do ID do APN. O comprimento máximo do índice é de 30 caracteres.

17. Na lista suspensa **Stack de IP**, selecione o stack IP usado na interface de rede:

    - **IPv4**, para usar o stack de protocolo IPv4 na interface de rede. Essa é a configuração padrão.
    - **IPv6**, para usar o stack de protocolo IPv6 na interface de rede.
    - **Stack dual (IPv4 e IPv6)**, para usar o dual stack IPv4 e IPv6 na interface de rede.

18. Limpe a caixa de seleção **IPv4 via DHCP** caso não deseje atribuir um endereço IPv4 à interface de rede via DHCP. Para marcar essa caixa de seleção simultaneamente com a caixa de seleção **IPv6 via DHCP**, selecione **Stack dual (IPv4 e IPv6)** (para dual stack) na lista suspensa **Stack de IP**. Esta caixa de seleção é selecionada por padrão.

19. Marque a caixa de seleção **IPv6 via DHCP** para atribuir um endereço IPv6 à interface de rede via DHCP. Para marcar essa caixa de seleção simultaneamente com a caixa de seleção **IPv4 via DHCP**, selecione **Stack dual (IPv4 e IPv6)** na lista suspensa **Stack de IP**. Esta caixa de seleção está desmarcada por padrão.

20. Limpe a caixa de seleção **Conexão automática** caso não deseje que o modem se conecte automaticamente à rede. Esta caixa de seleção é selecionada por padrão.

21. No campo **PLMN**, insira o ID PLMN do provedor de serviços. Os três primeiros dígitos do ID PLMN são o MCC (Código de país móvel) e os dois ou três dígitos seguintes são o MNC (Código de rede móvel). Por exemplo, para a rede Vimpelcom no território russo, PLMN = 25099: MCC = 250 (Federação Russa), MNC = 99 (Vimpelcom).

22. No campo **Tempo esgotado**, insira o tempo, em segundos, para a interface de rede aguardar a conclusão das operações do cartão SIM no modem. Valor máximo: 20. O valor padrão é `10`.

23. No campo **Porta serial**, insira o nome da porta serial do modem. O comprimento máximo do nome é de 50 caracteres.

24. Se necessário, no campo **Métrica de roteamento**, insira a métrica de roteamento padrão para a interface de rede. O dispositivo CPE usa o roteamento padrão com a métrica mais baixa.

    A métrica de roteamento para interfaces de rede com aliases **sdwan0**–**sdwan3** é atribuída automaticamente na inicialização do CPE: a **sdwan0** obtém a prioridade mais alta e a prioridade mais baixa vai para **sdwan3.** Nesse caso, o dispositivo CPE usa o roteamento padrão da interface de rede **sdwan0**. Se a interface de rede **sdwan0** falhar, o roteamento padrão da interface de rede **sdwan1** é então usado, seguido pela rota padrão da interface de rede **sdwan2**. O valor no campo **Métrica de roteamento** está bloqueado para edição manual para interfaces com os aliases **sdwan0**–**sdwan9**.

    A métrica é calculada automaticamente a partir dos seguintes atributos:

    - `1–4` se não houver erros e houver acesso à Internet
    - `11–14` se não houver erros e não houver acesso à Internet
    - `21–24` se houver erros e não houver acesso à Internet.

    As métricas são atribuídas automaticamente às interfaces dependendo do número final da alias da interface, de acordo com o seguinte esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

25. Clique em **Criar**.

    A interface de rede é criada e exibida na tabela.

26. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Criar uma interface de rede para estabelecer conexão com um servidor PPPoE

Para criar uma interface de rede para estabelecer conexão com um servidor PPPoE

1. Crie uma interface de rede de uma das seguintes formas:

   - Para criar uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE**, clique no modelo de CPE e selecione a guia **Rede**.
   - Para criar uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Rede**.

   A tabela de interfaces de rede é exibida.

2. Clique em **+ Interface de rede**.

3. Na janela aberta, no campo **Alias**, insira o nome da interface de rede para mapeá-la para uma porta OpenFlow. É necessário especificar esse nome de interface de rede ao criar uma interface SD-WAN do tipo WAN. O comprimento máximo do nome é de 15 caracteres.

4. Para adicionar uma interface de rede a uma zona de firewall, na lista suspensa **Zona**, selecione a zona de firewall criada.

5. No campo **Nome da interface**, insira o nome da porta física ou interface virtual do sistema operacional do dispositivo CPE. O comprimento máximo do nome é de 256 caracteres. Por exemplo, é possível inserir `eth0`, `eth1`, `eth2` ou `tun0`. Para criar uma ponte de várias interfaces, insira os nomes delas separados por espaços.

   Para atribuir uma tag de VLAN externa a uma interface de rede, insira um ponto (.) após o nome da porta física ou interface virtual do sistema operacional e, em seguida, insira a tag de VLAN externa. Por exemplo, `eth2.150`.

6. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: de 1 a 65535. Na lista suspensa **Protocolo**, selecione **PPPoE**.

7. No campo **Concentrador de acesso**, insira o endereço IP ou o nome do host do concentrador de acesso a que a interface de rede se conecta. O comprimento máximo do nome do host é de 30 caracteres. Se não for inserido um valor nesse campo, o Point-to-Point Protocol Daemon (PPPD) usa o primeiro concentrador de acesso que detectar.

8. No campo **Serviço**, insira o nome do serviço PPPoE a que a interface de rede se conecta. O comprimento máximo do nome é de 30 caracteres. Se não for inserido um valor nesse campo, o PPPD usa o primeiro serviço PPPoE detectado.

9. Na lista suspensa **Tipo de autenticação**, selecione que autenticação é usada na interface de rede:

    - **PAP e CHAP**, se a autenticação PAP e CHAP for usada na interface de rede. Ao selecionar essa opção, faça o seguinte:

        a. No campo **Nome de usuário para autenticação PAP/CHAP**, insira o nome de usuário para autenticação PAP/CHAP. O comprimento máximo do nome é de 30 caracteres.

        b. No campo **Senha para autenticação PAP/CHAP**, insira a senha para a autenticação PAP/CHAP. O comprimento máximo da senha é de 30 caracteres.

    - **Nenhum** significa que não é usada autenticação na interface de rede.

10. No campo **Máximo de pings malsucedidos**, insira o número de solicitações ICMP malsucedidas deve ocorrer antes que a interface de rede considere o servidor PPPoE indisponível. Intervalo de valores: 1 a 3600. O valor padrão é `5`.

11. No campo **Intervalo entre pings (s)**, insira o intervalo, em segundos, que a interface de rede deve esperar antes de enviar solicitações ICMP ao servidor PPPoE. Intervalo de valores: 1 a 3600. O valor padrão é `1`.

12. Para que a interface de rede encerre uma conexão PPPoE inativa após o tempo especificado, no campo **Tempo limite (s)**, insira o tempo em segundos. Intervalo de valores: 1 a 3600.

13. Se necessário, no campo **Host-Uniq**, insira a tag Host-Uniq para a conexão PPPoE. O comprimento máximo da tag é de 30 caracteres. Se não for inserido um valor nesse campo, o valor da tag Host-Uniq será igual ao do identificador do processo PPPD.

14. No campo **Substituir MTU**, insira a MTU para a interface de rede. O valor inserido substitui a MTU padrão.

15. Se necessário, no campo **Métrica de roteamento**, insira a métrica de roteamento padrão para a interface de rede. O dispositivo CPE usa o roteamento padrão com a métrica mais baixa.

    A métrica de roteamento para interfaces de rede com aliases **sdwan0**–**sdwan3** é atribuída automaticamente na inicialização do CPE: a **sdwan0** obtém a prioridade mais alta e a prioridade mais baixa vai para **sdwan3.** Nesse caso, o dispositivo CPE usa o roteamento padrão da interface de rede **sdwan0**. Se a interface de rede **sdwan0** falhar, o roteamento padrão da interface de rede **sdwan1** é então usado, seguido pela rota padrão da interface de rede **sdwan2**. O valor no campo **Métrica de roteamento** está bloqueado para edição manual para interfaces com os aliases **sdwan0**–**sdwan9**.

    A métrica é calculada automaticamente a partir dos seguintes atributos:

    - `1–4` se não houver erros e houver acesso à Internet
    - `11–14` se não houver erros e não houver acesso à Internet
    - `21–24` se houver erros e não houver acesso à Internet.

    As métricas são atribuídas automaticamente às interfaces dependendo do número final da alias da interface, de acordo com o seguinte esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

16. Se necessário, desmarque as seguintes caixas de seleção:

    - Desmarque a caixa de seleção **Keepalive adaptativo** se desejar que uma interface de rede que não recebeu pacotes de controle do Protocolo de controle de link (LCP) do servidor PPPoE encerre a conexão PPPoE, mesmo se o tráfego tiver vindo do servidor PPPoE.
    - Desmarque a caixa de seleção **Usar rota padrão** caso não queira usar a rota obtida do servidor PPPoE como a rota padrão na interface de rede.
    - Desmarque a caixa de seleção **Servidor DNS atribuído por par** caso não queira que a interface de rede use servidores DNS atribuídos a seus vizinhos.

    Por padrão, as caixas de seleção são marcadas.

17. Para passar argumentos de linha de comando adicionais ao iniciar o PPPD (Point-to-Point Protocol Daemon), no campo **PPPD**, insira os argumentos da linha de comando. Por exemplo, é possível passar parâmetros de autenticação, endereços IP e scripts para o PPPD.

18. Se necessário, especifique um servidor DNS para a interface de rede:

    a. Em **Servidores DNS**, clique em **+ Adicionar**.

    b. No campo exibido, insira o endereço IP do servidor DNS.

    O servidor DNS é especificado e exibido na seção **Servidores DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique no ícone de exclusão ✕ ao lado dele.

19. Clique em **Criar**.

    A interface de rede é criada e exibida na tabela.

20. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Criar uma interface de rede sem um endereço IP

Para criar uma interface de rede sem um endereço IP:

1. Crie uma interface de rede de uma das seguintes formas:

    - Para criar uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE**, clique no modelo de CPE e selecione a guia **Rede**.
    - Para criar uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Rede**.

    A tabela de interfaces de rede é exibida.

2. Clique em **+ Interface de rede**.

3. Na janela aberta, no campo **Alias**, insira o nome da interface de rede para mapeá-la para uma porta OpenFlow. É necessário especificar esse nome de interface de rede ao criar uma interface SD-WAN do tipo WAN. O comprimento máximo do nome é de 15 caracteres.

4. Para adicionar uma interface de rede a uma zona de firewall, na lista suspensa **Zona**, selecione a zona de firewall criada.

5. No campo **Nome da interface**, insira o nome da porta física ou interface virtual do sistema operacional do dispositivo CPE. O comprimento máximo do nome é de 256 caracteres. Por exemplo, é possível inserir `eth0`, `eth1`, `eth2` ou `tun0`. Para criar uma ponte de várias interfaces, insira os nomes delas separados por espaços.

   Para atribuir uma tag de VLAN externa a uma interface de rede, insira um ponto (.) após o nome da porta física ou interface virtual do sistema operacional e, em seguida, insira a tag de VLAN externa. Por exemplo, `eth2.150`.

6. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535. Para criar uma ponte a partir de interfaces físicas ou virtuais cujos nomes estão especificados no campo **Nome da interface**:

   a. Marque a caixa de seleção **Ponte**. Esta caixa de seleção está desmarcada por padrão.

   b. Para usar o STP na ponte para evitar loops de roteamento, selecione a caixa de seleção **STP**. Esta caixa de seleção está desmarcada por padrão.

   c. No campo **Idade (s)**, insira o tempo, em segundos, durante o qual os registros dinâmicos são armazenados na tabela MAC da ponte. Para usar a ponte como um hub, insira `0` nesse campo. Intervalo de valores: 0 a 86.400.

7. Para ativar o protocolo NetFlow na interface de rede, marque a caixa de seleção **NetFlow**. Esta caixa de seleção está desmarcada por padrão.

8. Se necessário, no campo **Índice de interface NetFlow**, insira um ID numérico permanente para a interface a ser usada ao enviar estatísticas através do protocolo NetFlow. Intervalo de valores: 1 a 65.535.

9. Na lista suspensa **Protocolo**, selecione **Nenhum**.

10. Para estabelecer uma conexão L2 entre dispositivos CPE, marque a caixa de seleção **Modo L2**. Quando a caixa de seleção é marcada, uma porta OpenFlow mapeada para a interface de rede é criada automaticamente no switch virtual do dispositivo CPE. Esta caixa de seleção está desmarcada por padrão. Não é possível marcar essa caixa de seleção nos seguintes casos:

    - Uma das seguintes caixas de seleção foi marcada ao criar a interface de rede:
        - **Ponte**
        - **NetFlow**
        - **Forçar endereço IP, rota e gateway**
    - A interface de rede é usada em uma rota estática.
    - A interface de rede é usada pelo BGP.
    - A interface de rede é usada pelo protocolo OSPF.
    - A interface de rede é usada pelo protocolo VRRP.
    - A interface de rede é usada para transmitir o tráfego multicast.

- A interface de rede é usada por uma tabela de roteamento e encaminhamento virtual (VRF).
- A interface de rede é usada para o diagnóstico do dispositivo CPE usando o utilitário ping, traceroute, tcpdump ou sweep.

Ao marcar essa caixa de seleção, a porta OpenFlow criada automaticamente no switch virtual do dispositivo CPE é exibida no campo **Porta OpenFlow**. É possível alterar o número da porta OpenFlow. Intervalo de valores: 11 a 20.

11. Caso deseje que a interface de rede seja ativada automaticamente quando o dispositivo CPE for ativado, marque a caixa de seleção **Ativa automaticamente**. Esta caixa de seleção está desmarcada por padrão.
12. Para que um endereço IP, uma rota e um gateway padrão sejam atribuídos automaticamente à interface de rede, marque a caixa de seleção **Forçar endereço IP, rota e gateway**. Esta caixa de seleção está desmarcada por padrão.
13. No campo **Substituir MAC**, insira o endereço MAC da interface de rede. O valor inserido substitui o endereço MAC real da interface de rede.
14. No campo **Substituir MTU**, insira a MTU para a interface de rede. O valor inserido substitui a MTU padrão.
15. Clique em **Criar**.

    A interface de rede é criada e exibida na tabela.
16. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma interface de rede

É possível editar uma interface de rede em um modelo de CPE ou dispositivo CPE. Uma interface de rede editada no modelo de CPE é editada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma interface de rede:

1. Edite uma interface de rede de uma das seguintes formas:
   - Para editar uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Rede**.
   - Para editar uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Rede**. Para editar uma interface de rede herdada do modelo de CPE, marque a caixa de seleção **Substituir** ao lado da interface de rede.

   A tabela de interfaces de rede é exibida.
2. Clique em **Editar** ao lado da interface de rede que deseja editar.
3. Na janela aberta, se necessário, edite as configurações da interface de rede. Para obter uma descrição das configurações, consulte as instruções para criar uma interface de rede.

4. Clique em **Salvar**.

   A interface de rede é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Desativar ou ativar uma interface de rede

É possível desativar ou ativar uma interface de rede em um modelo de CPE ou dispositivo CPE. Uma interface de rede ativada ou desativada em um modelo de CPE é ativada ou desativada automaticamente em todos os dispositivos CPE que usam o modelo.

Para desativar ou ativar uma interface de rede:

1. Desative ou ative uma interface de rede de uma das seguintes formas:

   - Para ativar ou desativar uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Rede**.
   - Para ativar ou desativar uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN** do menu, clique no dispositivo CPE e selecione a guia **Rede**. Para desativar ou ativar uma interface de rede herdada do modelo de CPE, marque a caixa de seleção **Substituir** ao lado da interface de rede.

   A tabela de interfaces de rede é exibida.

2. Clique em **Desativar** ou **Ativar** ao lado da interface de rede que deseja desativar ou ativar.

   A interface de rede é desativada ou ativada.

3. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Cancelar a aplicação de configurações da interface de rede em um dispositivo CPE

Caso não deseje aplicar as configurações da interface de rede em um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN**→ **CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual não deseja aplicar as configurações da interface de rede.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Rede**.

   A tabela de interfaces de rede é exibida.

4. Marque a caixa de seleção **Ignorar configurações de rede**. Esta caixa de seleção está desmarcada por padrão.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

   As configurações da interface de rede não são aplicadas no dispositivo CPE.

Para aplicar as configurações da interface de rede no dispositivo CPE, desmarque a caixa de seleção **Ignorar configurações de rede**.

Excluir uma interface de rede

É possível excluir uma interface de rede em um modelo de CPE ou dispositivo CPE. Uma interface de rede excluída no modelo de CPE é excluída automaticamente em todos os dispositivos CPE que usam o modelo. Não é possível excluir uma interface de rede herdada de um modelo de CPE em um dispositivo CPE.

As interfaces de rede excluídas não podem ser restauradas.

Para excluir uma interface de rede:

1. Exclua a interface de rede de uma das seguintes formas:

   - Para excluir uma interface de rede em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Rede**.
   - Para excluir uma interface de rede em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Rede**.

   A tabela de interfaces de rede é exibida.

2. Clique em **Excluir** ao lado da interface de rede que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A interface de rede é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Proteção contra Spoofing de IP usando uRPF

Essa função permite mitigar o impacto de ataques de Spoofing de IP usando o algoritmo Unicast Reverse Path Forwarding (uRPF) em interfaces CPE.

Princípio de operação do uRPF

O algoritmo usa a tabela de roteamento e encaminhamento da base de informações de encaminhamento (FIB) para verificar os pacotes da seguinte forma:

1. Receber um pacote.

   O roteador recebe um pacote em uma interface.

2. Verificar a origem.

   O uRPF verifica o endereço IP de origem do pacote.

3. Fazer pesquisa reversa.

   O roteador procura, na tabela FIB, a interface que usaria para enviar um pacote de resposta a esta origem (caminho de retorno).

4. Processar o pacote. Outras ações dependem do modo de operação selecionado do uRPF:

   - Modo estrito

     O pacote deve chegar exatamente pela interface que representa o melhor caminho de retorno para a origem. Se o caminho não corresponder, o pacote será descartado.

     O modo estrito é usado para proteger contra Spoofing de IP no perímetro de redes com roteamento simétrico.

   - Modo livre

     Um pacote é aceito se a tabela de roteamento e encaminhamento tiver pelo menos alguma rota para a origem, independentemente da interface.

     O modo livre pode ser usado em redes com roteamento assimétrico (quando o caminho de "ida" é diferente do caminho de "volta").

Você pode configurar o uRPF independentemente para cada interface de rede do dispositivo CPE. O uRPF pode ser usado em interfaces comuns e também em interfaces de ponte.

O uRPF está disponível para interfaces com os protocolos "Cliente DHCP"/"Endereço IPv4 estático"/"QMI"/"PPPoE" e não está disponível para interfaces com os protocolos "Endereço IPv6 estático"/"Nenhum".

Você pode configurar o uRPF em dispositivos CPE ou em modelos de CPE.

Para configurar o uRPF:

1. Configure o uRPF de uma das seguintes formas:

   - Para configurar o uRPF em um dispositivo CPE, no menu do orquestrador, acesse a seção **SD-WAN**, selecione o dispositivo CPE e acesse a seção **Rede** nas configurações.

   - Para configurar o uRPF em um modelo de CPE, no menu do orquestrador, acesse a seção `Modelos de CPE`, selecione o modelo de CPE e acesse a seção **Rede** nas configurações.

2. Crie uma nova interface de rede ou edite uma existente.

   Se a interface for usada no modelo de CPE, ative o botão de alternância **Substituir** para ela.

3. Se estiver criando uma nova interface de rede, selecione um dos protocolos compatíveis na lista suspensa **Protocolo**:

   - **Cliente DHCP**
   - **Endereço IPv4 estático**
   - **QMI**
   - **PPPoE**

4. Na lista suspensa do **modo uRPF**, selecione o modo desejado:

   - **Rígido**
   - **Loose**

5. Salve as configurações da interface de rede.

6. Aplique as alterações no dispositivo ou modelo de CPE.

Gerenciar interfaces SD-WAN

Interfaces SD-WAN são interfaces lógicas sobre as interfaces de rede do dispositivo CPE e portas OpenFlow do switch virtual, que formam um nível adicional de abstração. Cada interface SD-WAN é mapeada para uma interface de rede pelo nome da interface de rede e uma porta OpenFlow pelo número da porta OpenFlow. Os seguintes tipos de interfaces SD-WAN são possíveis:

- As interfaces SD-WAN do tipo LAN são interfaces criadas por padrão e mapeadas para interfaces de rede conectadas à LAN. Não é possível excluir e criar uma interface SD-WAN do tipo LAN, mas é possível editá-la para especificar a velocidade máxima e configurar filas de tráfego.
- As interfaces SD-WAN do tipo WAN são interfaces mapeadas para interfaces de rede conectadas à WAN.
- Uma interface SD-WAN do tipo de gerenciamento é uma interface SD-WAN criada por padrão e mapeada para uma interface de rede usada pelo sistema de monitoramento Zabbix para o monitoramento passivo do dispositivo CPE, bem como pelo orquestrador para estabelecer conexão com o dispositivo CPE por meio de SSH. Não é possível excluir e criar uma interface SD-WAN do tipo de gerenciamento.

Para visualizar a tabela de interfaces SD-WAN em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de interfaces SD-WAN em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **SD-WAN → Interfaces**.
- Para visualizar a tabela de interfaces SD-WAN em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **SD-WAN → Interfaces**.

As informações sobre as interfaces SD-WAN são exibidas nas seguintes colunas da tabela:

- **Tipo** é o tipo da interface SD-WAN:
  - **WAN**
  - **LAN**
  - **Gerenciamento**
- **Herdado** indica se a interface SD-WAN é herdada de um modelo de CPE:
  - **Sim**.
  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.
- **Porta** é o número da porta OpenFlow.
- **Alias** é o nome da interface de rede.
- **Taxa máxima** é a velocidade máxima da interface SD-WAN em Mbps.

Informações adicionais sobre as verificações da WAN às quais as interfaces SD-WAN do tipo WAN estão conectadas são exibidas nas seguintes colunas da tabela:

- **Endereço IP para rastreamento** são os endereços IP dos hosts para verificar a disponibilidade da WAN.
- **Confiabilidade** é o número mínimo de verificações bem-sucedidas que tornam a WAN disponível.
- **Contagem** é o número de solicitações aos hosts em uma verificação da WAN.
- **Tempo esgotado** é o tempo de espera por uma resposta dos hosts, em milissegundos.
- **Intervalo (s)** é o intervalo de tempo em segundos para a verificação da WAN.
- **Para baixo** é o número de verificações malsucedidas que tornam a WAN indisponível.
- **Para cima** é o número de verificações bem-sucedidas que tornam a WAN disponível.
- **Monitoramento de velocidade** indica se a velocidade da interface SD-WAN do tipo WAN está sendo medida:
  - **Sim**.
  - **Não**.

Sobre o envio de informações sobre interfaces SD-WAN do tipo WAN para o controlador

Ao criar ou editar interfaces SD-WAN do tipo WAN, é possível especificar que informações devem ser enviadas ao controlador.

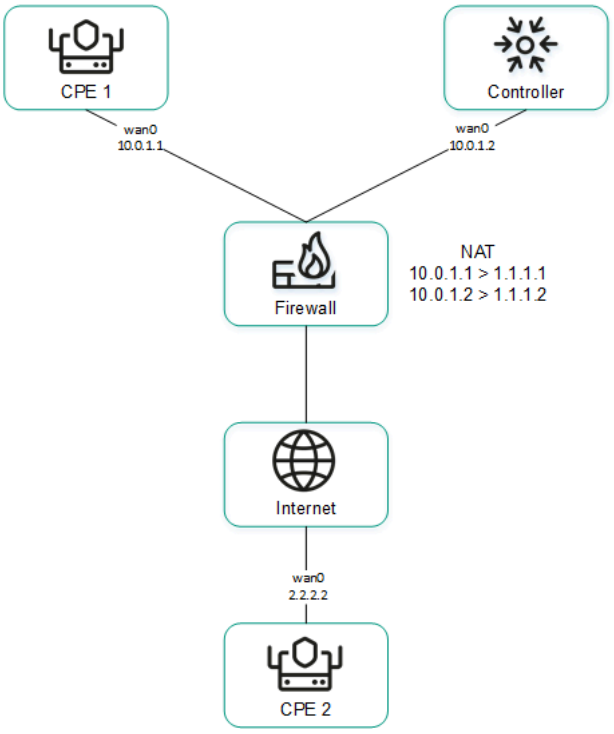
Enviar endereços IP públicos e portas UDP de interfaces SD-WAN ao controlador

Para estabelecer links entre dispositivos CPE, o controlador deve obter informações sobre os endereços IP públicos de interfaces SD-WAN do tipo WAN. Por padrão, o controlador obtém essas informações por meio de uma sessão de gerenciamento. Nesse caso, o endereço IP de origem é usado como endereço IP público.

É possível especificar manualmente os endereços IP e as portas UDP das interfaces SD-WAN do tipo WAN. Na figura abaixo, o CPE 1 e o controlador estão na mesma rede local e obtêm acesso à Internet por meio do mesmo firewall que faz o encaminhamento de endereços IP.

Ao estabelecer uma sessão entre a interface SD-WAN do tipo WAN do CPE 1 e o endereço IP público do controlador (1.1.1.2), se o firewall não puder ser configurado de forma que envolva o encaminhamento pelo Controlador do endereço IP privado para o endereço IP público (10.0.1.1 > 1.1.1.1), o Controlador não consegue obter informações sobre o endereço IP público da interface SD-WAN do tipo WAN e fornecê-las a outros dispositivos CPE na topologia (CPE 2).

Como resultado, não é possível criar um link entre o CPE 1 e o CPE 2; o CPE 1 fica isolado e não pode ser adicionado ao plano de controle comum.



O CPE 1 e o controlador estão atrás do NAT e conectados ao CPE 2

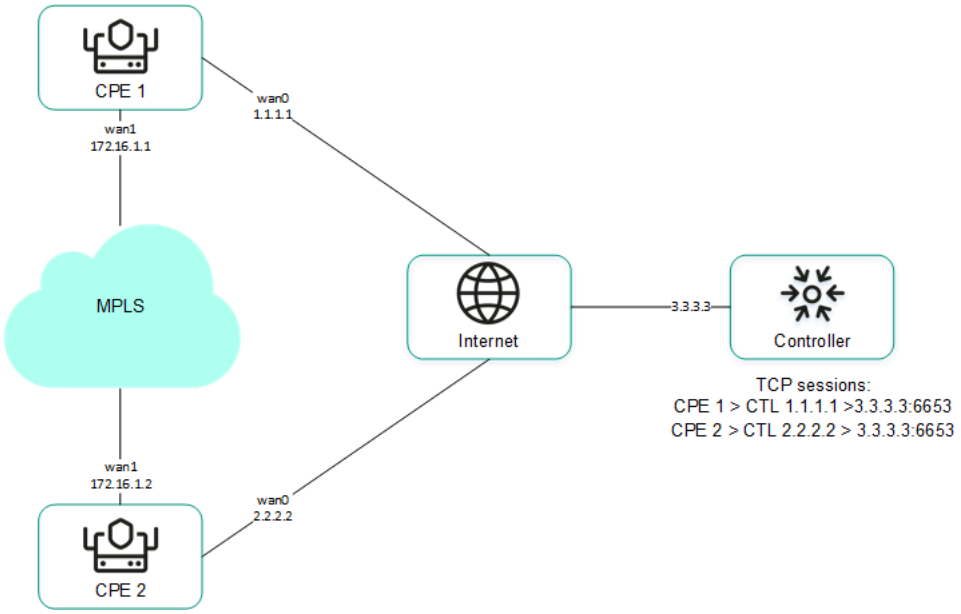
Enviar endereços IP de interfaces SD-WAN do tipo WAN localizadas em uma rede isolada para o controlador

As interfaces SD-WAN do tipo WAN podem estar em uma rede isolada sem a possibilidade de estabelecer uma sessão de gerenciamento com o controlador, mas podem ser usadas para estabelecer links. Nesse caso, o controlador não pode obter informações sobre os endereços IP de interfaces SD-WAN do tipo WAN isoladas e usá-las para estabelecer links entre dispositivos CPE.

Na figura abaixo, o CPE 1 e o CPE 2 têm duas interfaces SD-WAN do tipo WAN cada, mas podem estabelecer uma sessão de gerenciamento com o controlador apenas por wan0 porque wan1 está em uma rede isolada (MPLS) que não tem acesso ao controlador. No entanto, ambas as interfaces wan1 podem ser usadas para estabelecer links.

Se o link usado para interagir com o controlador falhar para um dos dispositivos CPE, todos os outros links também não poderão ser usados, mesmo se permanecerem operacionais, pois o controlador exclui o dispositivo da topologia.

Os endereços IP de interfaces SD-WAN do tipo WAN isoladas são enviados ao controlador por meio do orquestrador.



O CPE 1 e o CPE 2 estão conectados um ao outro por meio de MPLS e ao controlador por meio da Internet.

Fragmentação de pacotes

O Kaspersky SD-WAN verifica se os dispositivos CPE são compatíveis com a fragmentação de pacotes de tráfego. Um teste de fragmentação de pacotes é iniciado automaticamente. Quando cada dispositivo CPE é ativado, ele envia duas solicitações ICMP para os endereços IP especificados ao criar ou editar interfaces SD-WAN do tipo WAN.

As solicitações ICMP têm tamanho de pacote de 1600 bytes. Se pelo menos uma das solicitações ICMP receber uma resposta, conclui-se que o dispositivo CPE é compatível com a fragmentação de pacotes. É possível visualizar o resultado do teste de fragmentação na coluna **Fragmentação** da tabela de dispositivos CPE ou da tabela de links.

Filas de tráfego em interfaces SD-WAN

No máximo 8 filas de tráfego podem ser usadas em interfaces SD-WAN. Para cada fila de tráfego, especifique a largura de banda mínima e máxima como uma porcentagem da largura de banda total definida para a interface SD-WAN. A soma total de todos os valores mínimos de largura de banda especificados para filas de tráfego não pode exceder 100%.

As filas de tráfego têm prioridade estrita e a largura de banda não reservada é oferecida primeiro ao tráfego da fila com prioridade mais alta. Cada fila de tráfego tem garantida certa largura de banda mínima de acordo com seu valor de largura de banda mínimo especificado. Um limite superior na largura de banda máxima para filas de prioridade mais alta é necessário para permitir que o tráfego de filas de tráfego de prioridade mais baixa ainda seja transmitido.

É possível configurar filas de tráfego ao criar uma interface SD-WAN do tipo WAN ou editar uma interface SD-WAN.

Os provedores de serviço podem usar políticas de qualidade de serviço diferentes para marcar filas de tráfego em suas redes e atender aos requisitos de SLA para a passagem do tráfego do cliente. Portanto, ao estabelecer conexões simultâneas com redes de diferentes provedores de serviço, os dispositivos CPE podem refazer a rotulagem do tráfego de diferentes filas para cada interface SD-WAN do tipo WAN. Para configurar a nova rotulagem, altere o valor do tipo de serviço (ToS) ao configurar filas de tráfego em uma interface SD-WAN.

Só é possível alterar os valores de ToS de cabeçalhos externos de pacotes de tráfego originados de interfaces SD-WAN do tipo WAN. Os valores de ToS de cabeçalhos internos de pacotes de tráfego não podem ser editados.

Criar uma interface SD-WAN do tipo WAN

É possível criar uma interface SD-WAN do tipo WAN em um modelo de CPE ou em um dispositivo CPE. Interfaces SD-WAN do tipo WAN criadas em um modelo de CPE são criadas automaticamente em todos os dispositivos CPE que estão usando o modelo.

Para criar uma interface SD-WAN do tipo WAN:

1. Crie uma interface SD-WAN do tipo WAN de uma das seguintes formas:

   - Para criar uma interface SD-WAN do tipo WAN em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **SD-WAN** → **Interfaces**.
   - Para criar uma interface SD-WAN do tipo WAN em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **SD-WAN** → **Interfaces**.

   Uma tabela de interfaces SD-WAN é exibida.

2. Clique em **+ Adicionar**.
3. Na janela aberta, no campo **Porta OpenFlow**, insira o número da porta OpenFlow sendo criada no switch virtual.
4. No campo **Interface (alias)**, insira o codinome da interface de rede criada, para a qual a interface SD-WAN do tipo WAN está mapeada.
5. No campo **Taxa máxima**, insira a velocidade máxima da interface SD-WAN do tipo WAN em Mbps. Intervalo de valores: 1 a 100.000. O valor padrão é `1000`.

6. Configure a verificação de disponibilidade da WAN à qual a interface SD-WAN do tipo WAN está conectada:

   a. Especifique o host para verificar a disponibilidade da WAN. Para isso, em **Endereço IP para rastreamento**, insira o endereço IP do host e clique em **+ Adicionar**.

      O host é especificado e exibido em **Endereço IP para rastreamento**. É possível especificar vários hosts ou excluir hosts. Para excluir um host, clique no ícone de exclusão ✕ ao lado dele.

   b. No campo **Endereço IP para verificar a fragmentação**, insira o endereço IPv4 do host até o qual o suporte à fragmentação é verificado. Valor padrão: `1.1.1.1`.

   c. No campo **Confiabilidade**, insira o número mínimo de verificações bem-sucedidas que tornam a WAN disponível. O valor padrão é `1`.

      O número de hosts não deve exceder o número de endereços IP especificados em **Endereço IP para rastreamento**. Caso contrário, a WAN sempre será considerada indisponível.

   d. No campo **Intervalo (s)**, insira o intervalo de tempo em segundos para a verificação da WAN. Intervalo de valores: 1 a 600. O valor padrão é `2`.

   e. No campo **Contagem**, insira o número de solicitações aos hosts em uma verificação da WAN. Intervalo de valores: 1 a 600. O valor padrão é `2`.

   f. No campo **Tempo esgotado**, insira o tempo de espera por uma resposta dos hosts, em milissegundos. Intervalo de valores: 1 a 100.000. O valor padrão é `2000`.

   g. No campo **Para baixo**, insira o número de verificações malsucedidas que tornam a WAN indisponível. Intervalo de valores: 1 a 600. O valor padrão é `3`.

   h. No campo **Para cima**, insira o número de verificações bem-sucedidas que tornam a WAN disponível. Intervalo de valores: 1 a 600. O valor padrão é `2`.

   i. Na lista suspensa **Monitoramento de velocidade**, selecione se a velocidade da interface SD-WAN do tipo WAN está sendo medida:

      - **Sim**.
      - **Não**. Essa é a configuração padrão.

7. Para configurar filas de tráfego na interface SD-WAN do tipo WAN:

   a. Selecione a guia **QoS**.

      Uma tabela de filas de tráfego é exibida.

   b. Na coluna **Remapear ToS**, selecione o valor Tipo de Serviço de cabeçalhos externos de pacotes de tráfego para cada fila.

   c. Na coluna **Taxa mínima (%)**, especifique a largura de banda mínima do tráfego para a fila na forma de uma porcentagem da velocidade máxima da interface SD-WAN do tipo WAN. A soma total de uma coluna não pode exceder 100.

   d. Na coluna **Taxa máxima (%)**, especifique a largura de banda máxima do tráfego para a fila na forma de uma porcentagem da velocidade máxima da interface SD-WAN do tipo WAN. Essa configuração é usada para impedir que o tráfego de filas de alta prioridade impeça indefinidamente o tráfego de filas de baixa prioridade.

A velocidade máxima da interface SD-WAN do tipo WAN é especificada na etapa 5 destas instruções.

8. Para configurar o envio de informações sobre a interface SD-WAN do tipo WAN para o controlador:

   a. Selecione a guia **Underlay WAN independente e NAT**.

   b. Na lista suspensa **Estado**, selecione um dos seguintes valores:

      - Desativado para que as informações sobre a interface SD-WAN do tipo WAN não sejam enviadas ao controlador. Essa é a configuração padrão.
      - **NAT/PAT** se a interface SD-WAN do tipo WAN estiver atrás do NAT ou PAT e precisar da atribuição de um endereço IP e um número de porta UDP, que devem ser enviados ao controlador.
      - **Underlay WAN independente**significa que a interface SD-WAN do tipo WAN está conectada a uma rede isolada e o endereço IP da interface SD-WAN do tipo WAN deve ser passado ao controlador.

   c. Caso tenha selecionado **NAT/PAT** na lista suspensa **Estado**, siga estas etapas:

      1. No campo **Endereço IP real**, insira o endereço IPv4 público da interface SD-WAN do tipo WAN.
      2. No campo **Porta UDP GENEVE real**, insira o número da porta UDP da interface SD-WAN do tipo WAN. Intervalo de valores: 1 a 65.535.

   d. Caso tenha selecionado **Underlay WAN independente** na lista suspensa **Estado**, insira o endereço IPv4 da interface SD-WAN do tipo WAN no campo **Endereço IP**.

   e. Se necessário, substitua a tabela de roteamento e encaminhamento virtual para a interface SD-WAN do tipo WAN. Para isso, ative o botão **Atribuir VRF** e, em seguida, na lista suspensa **VRF**, selecione uma tabela de roteamento e encaminhamento virtual.

      A substituição do VRF permite configurar uma rota alternativa para a comunicação com o controlador. Por exemplo, é possível usar uma interface do tipo LAN em vez da WAN padrão. O valor especificado na lista **VRF** entra em vigor somente após reiniciar o CPE ou desativar e ativar a interface de rede correspondente.

9. Se as interfaces SD-WAN do tipo WAN do dispositivo CPE estiverem conectadas a redes diferentes, por exemplo, a Internet e uma rede MPLS privada, é possível alterar os endereços IP e os números de porta TCP dos nós do controlador em uma interface SD-WAN do tipo WAN individual. Para isso, execute as seguintes ações:

   a. Selecione a guia **Controladores**.

   b. Marque a caixa de seleção **Reescrever endereço IP/porta de controladores**. Esta caixa de seleção está desmarcada por padrão.

   c. Na lista suspensa **Número de controladores**, selecione o número de nós do controlador.

      Especifique o número de nós do controlador implementados ao implementar a instância SD-WAN. Caso contrário, ocorrerá um erro e as configurações não serão alteradas.

   d. No campo **Endereço IP**, insira o endereço IPv4 do nó do controlador. O número de campos corresponde ao valor selecionado na lista suspensa **Número de controladores**.

e. No campo **Porta**, insira o número da porta base do nó do controlador. Intervalo de valores: 1 a 65.535. O valor padrão é `6653`. O número de campos corresponde ao valor selecionado na lista suspensa **Número de controladores**.

Com a porta base do nó do controlador, as portas com os próximos três números consecutivos são especificadas automaticamente. Por exemplo, ao inserir `6653` como o número da porta base, as portas 6654, 6655 e 6656 serão especificadas automaticamente.

Para que as alterações tenham efeito, reinicie o dispositivo CPE após alterar os endereços IP e os números de porta TCP dos nós do controlador na interface SD-WAN do tipo WAN.

É possível alterar os endereços IP e os números de porta TCP dos nós do controlador ao configurar os nós do controlador de uma instância SD-WAN. Isso altera automaticamente os endereços IP e os números de porta TCP dos nós do controlador em todos os dispositivos CPE adicionados à instância SD-WAN. Os endereços IP e os números de porta TCP especificados em uma interface SD-WAN do tipo WAN individual têm precedência sobre os endereços IP e os números de porta TCP especificados ao configurar os nós do controlador da instância SD-WAN.

10. Se necessário, ative a função FEC na guia **Configurações de link**.

11. Clique em **Criar**.

    A interface SD-WAN do tipo WAN é criada e exibida na tabela.

12. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma interface SD-WAN

É possível editar uma interface SD-WAN em um modelo de CPE ou dispositivo CPE. Não é possível editar o nome de uma interface SD-WAN. Ao editar uma interface SD-WAN do tipo LAN, só é possível configurar a velocidade máxima e as filas de tráfego. Uma interface SD-WAN editada no modelo de CPE é editada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma interface SD-WAN:

1. Edite uma interface SD-WAN de uma das seguintes formas:

   - Para editar uma interface SD-WAN em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **SD-WAN → Interfaces**.

   - Para editar uma interface SD-WAN em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **SD-WAN → Interfaces**. Para editar uma interface SD-WAN herdada do modelo de CPE, marque a caixa de seleção **Substituir** ao lado da interface SD-WAN.

   Uma tabela de interfaces SD-WAN é exibida.

2. Clique em **Editar** ao lado da interface SD-WAN que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da interface SD-WAN. Para obter uma descrição das configurações, consulte as instruções para criar uma interface do tipo WAN.

4. Clique em **Salvar**.

   A interface SD-WAN é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Desativar ou ativar uma interface SD-WAN

É possível desativar ou ativar uma interface SD-WAN em um modelo de CPE ou dispositivo CPE. Uma interface SD-WAN ativada ou desativada em um modelo de CPE é ativada ou desativada automaticamente em todos os dispositivos CPE que usam o modelo.

Para desativar ou ativar uma interface SD-WAN:

1. Desative ou ative uma interface SD-WAN de uma das seguintes formas:

   - Para ativar ou desativar uma interface SD-WAN em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **SD-WAN → Interfaces**.
   - Para ativar ou desativar uma interface SD-WAN em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **SD-WAN → Interfaces**. Para desativar ou ativar uma interface SD-WAN herdada do modelo de CPE, marque a caixa de seleção **Substituir** ao lado da interface SD-WAN.

   Uma tabela de interfaces SD-WAN é exibida.

2. Clique em **Desativar** ou **Ativar** ao lado da interface SD-WAN que deseja desativar ou ativar.

   A interface SD-WAN é desativada ou ativada e atualizada na tabela.

3. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma interface SD-WAN do tipo WAN

É possível excluir uma interface SD-WAN do tipo WAN em um modelo de CPE ou em um dispositivo CPE. Uma interface SD-WAN do tipo WAN excluída em um modelo de CPE é excluída automaticamente em todos os dispositivos CPE que estão usando o modelo. Não é possível excluir uma interface SD-WAN herdada do modelo de CPE em um dispositivo CPE ou excluir uma interface SD-WAN do tipo LAN.

As interfaces SD-WAN do tipo WAN excluídas não podem ser restauradas.

Para excluir uma interface SD-WAN do tipo WAN:

1. Exclua uma interface SD-WAN do tipo WAN de uma das seguintes formas:

   - Para excluir uma interface SD-WAN do tipo WAN em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **SD-WAN → Interfaces**.

   - Para excluir uma interface SD-WAN do tipo WAN em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **SD-WAN → Interfaces**.

   Uma tabela de interfaces SD-WAN é exibida.

2. Clique em **Excluir** ao lado da interface SD-WAN do tipo WAN que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A interface SD-WAN do tipo WAN é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar interfaces de serviço

As interfaces de serviço são mapeadas para portas OpenFlow e usadas para conectar um dispositivo CPE aos serviços de transporte. Uma interface de serviço não pode ser mapeada para uma porta OpenFlow que já esteja mapeada para uma interface SD-WAN do tipo WAN.

Para filtrar pacotes de tráfego em uma interface de serviço, crie uma interface de Lista de Controle de Acesso (ACL) mapeada para essa interface de serviço. A interface ACL aplica o filtro de tráfego especificado à interface de serviço. Uma única interface de serviço pode ser mapeada para no máximo quatro interfaces ACL.

Para visualizar a tabela com as interfaces de serviço, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador e vá para a seção **Interfaces de serviço**. As informações sobre as interfaces de serviço são exibidas nas seguintes colunas da tabela:

- **Porta** é o número da porta OpenFlow para a qual a interface de serviço é mapeada.
- **Tipo** é o tipo de classificação de tráfego na interface de serviço.
  - **Acesso**
  - **VLAN**
  - **Q-in-Q**
  - **ACL**
- **Descrição** é uma breve descrição da interface de serviço.
- **VLAN** é a tag VLAN externa da interface de serviço. O valor nessa coluna só é exibido para interfaces de serviço com os tipos de classificação de tráfego **VLAN** e **Q-in-Q**.

- **VLAN interna** é a tag VLAN interna da interface de serviço. O valor nessa coluna só é exibido para interfaces de serviço com o tipo de classificação de tráfego **Q-in-Q**.
- **Filtrar** é o filtro de tráfego para a interface ACL. O valor nessa coluna só é exibido para interfaces de serviço com o tipo de classificação de tráfego **ACL**.
- **Nome** são as informações sobre a interface de serviço:
  - Nome e DPID do dispositivo CPE em que a interface de serviço foi criada
  - O número da porta OpenFlow para a qual a interface de serviço é mapeada

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar uma interface de serviço

Para criar uma interface de serviço:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Interfaces de serviço**.

   Uma tabela de interfaces de serviço e interfaces ACL é exibida.

4. Nas listas suspensas Switch e Porta, selecione o dispositivo CPE e a porta OpenFlow à qual a interface de serviço é mapeada.

5. Clique em **Criar**.

6. Na janela aberta, na lista suspensa **Tipo**, selecione o tipo de classificação de tráfego na interface de serviço:

   - **Acesso** Esse é o nível padrão.
   - **VLAN** Ao selecionar essa opção, no campo **ID da VLAN**, insira a tag VLAN externa da interface de serviço. Intervalo de valores: 1 a 4094.
   - **Q-in-Q**: ao selecionar essa opção, faça o seguinte:
     a. No campo **ID da VLAN**, insira a tag VLAN externa da interface de serviço. Intervalo de valores: 1 a 4094.
     b. No campo **ID da VLAN interna**, insira a tag VLAN interna da interface de serviço. Intervalo de valores: 1 a 4094.
   - **ACL** é usado ao criar uma interface ACL.

7. Se necessário, insira uma breve descrição da interface de serviço no campo **Descrição**.
8. Clique em **Criar**.

A interface de serviço é criada e exibida na tabela.

Criar uma interface ACL

Para criar uma interface ACL:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Interfaces de serviço**.

   Uma tabela de interfaces de serviço e interfaces ACL é exibida.

4. Nas listas suspensas **Switch** e **Porta**, selecione o dispositivo CPE e a porta OpenFlow para a qual a interface de serviço criada é mapeada.
5. Clique em **Criar**.
6. Na janela aberta, na lista suspensa **Tipo**, selecione **ACL**.
7. Na lista suspensa Interface de serviço, selecione a interface de serviço à qual a interface ACL é mapeada.
8. Na lista suspensa **Filtro de tráfego**, selecione o filtro de tráfego criado para a interface ACL. É possível usar o mesmo filtro de tráfego em várias interfaces ACL.
9. Na lista suspensa **Sequência**, selecione o número sequencial da interface ACL. O tráfego é direcionado primeiro para a interface ACL com o menor número. Se o filtro usado em uma interface ACL não receber o tráfego, o tráfego será enviado para a segunda interface ACL e assim por diante.

   Intervalo de valores: 1 a 4. Duas interfaces ACL com o mesmo número de série não podem ser mapeadas para a mesma interface de serviço.

10. Se necessário, insira uma breve descrição da interface ACL no campo **Descrição**.
11. Clique em **Criar**.

A interface ACL é criada e exibida na tabela.

Visualizar o uso de uma interface de serviço e uma interface ACL

Se necessário, é possível verificar quais serviços de transporte estão usando uma interface de serviço ou uma interface ACL. Por exemplo, uma interface de serviço ou ACL que está em uso não pode ser excluída.

Para ver se uma interface de serviço ou ACL está sendo usada:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Interfaces de serviço**.

   Uma tabela de interfaces de serviço e interfaces ACL é exibida.

4. Clique em **Gerenciamento** → **Mostrar utilização** ao lado da interface de serviço ou ACL cujas informações de uso deseja visualizar.

Isso abre uma janela com uma tabela de serviços de transporte que estão usando a interface de serviço ou a interface ACL.

Excluir uma interface de serviço ou uma interface ACL

Não é possível excluir uma interface de serviço ou uma interface ACL se ela estiver sendo usada por pelo menos um serviço de transporte. Para excluir uma interface de serviço ou interface ACL que está sendo usada por serviços de transporte, primeiro remova a interface de serviço ou interface ACL das configurações dos serviços de transporte. É possível verificar quais serviços de transporte estão usando uma interface de serviço ou uma interface ACL.

As interfaces de serviço e interfaces ACL excluídas não podem ser restauradas.

Para excluir uma interface de serviço ou uma interface ACL:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Interfaces de serviço**.

   Uma tabela de interfaces de serviço e interfaces ACL é exibida.

4. Clique em **Gerenciamento**→ **Excluir** ao lado da interface de serviço ou interface ACL que deseja excluir.

5. Na janela de confirmação, clique em **Excluir**.

A interface de serviço ou interface ACL é excluída e não é mais exibida na tabela.

Gerenciar grupos de portas OpenFlow

Portas OpenFlow são interfaces da SDN overlay criadas automaticamente junto com as interfaces SD-WAN. O controlador usa portas OpenFlow para controlar o tráfego de rede. É possível criar interfaces de serviço e UNIs mapeadas para portas OpenFlow.

As portas OpenFlow podem ser combinadas em grupos de portas OpenFlow e usadas ao criar serviços de transporte P2M e M2M. Quando um grupo de portas OpenFlow é adicionado a um serviço de transporte, isso automaticamente cria interfaces de serviço mapeadas para as portas OpenFlow e, em seguida, essas interfaces de serviço são adicionadas ao serviço de transporte. Usar grupos de portas OpenFlow elimina a necessidade de criar interfaces de serviço e adicioná-las aos serviços de transporte manualmente.

Para visualizar a tabela de grupos de portas OpenFlow, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Grupos de portas OpenFlow**. As informações sobre grupos de portas OpenFlow são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do grupo de portas OpenFlow.
- **Portas OpenFlow** são portas OpenFlow que foram adicionadas ao grupo de portas OpenFlow.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um grupo de portas OpenFlow

Para criar um grupo de portas OpenFlow:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Grupos de portas OpenFlow**.

   Uma tabela de grupos de portas OpenFlow é exibida.

4. Na parte superior da página, clique em **+ Grupo de portas OpenFlow**.

5. Na janela aberta, no campo **Nome**, insira o nome do grupo de portas OpenFlow.

6. Nas listas suspensas **Switch** e **Porta**, selecione o dispositivo CPE e a porta OpenFlow que deseja adicionar ao grupo de portas OpenFlow.

   É possível adicionar várias portas OpenFlow ou excluir portas OpenFlow. Para excluir uma porta OpenFlow, clique em **Excluir** ao lado dela.

7. Clique em **Criar**.

O grupo de portas OpenFlow é criado e exibido na tabela.

Editar um grupo de portas OpenFlow

Para editar um grupo de portas OpenFlow:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Grupos de portas OpenFlow**.

   Uma tabela de grupos de portas OpenFlow é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do grupo de portas OpenFlow que deseja editar.

5. Na janela aberta, se necessário, edite o nome do grupo de portas OpenFlow e adicione ou exclua portas OpenFlow.

6. Clique em **Salvar**.

O grupo de portas OpenFlow é modificado e atualizado na tabela.

Excluir um grupo de portas OpenFlow

Os grupos de portas OpenFlow excluídos não podem ser restaurados.

Para excluir um grupo de portas OpenFlow:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Grupos de portas OpenFlow**.

   Uma tabela de grupos de portas OpenFlow é exibida.

4. Clique em **Gerenciamento** → **Excluir** ao lado do grupo de portas OpenFlow que deseja excluir.

5. Na janela de confirmação, clique em **Excluir**.

O grupo de portas OpenFlow é excluído e não é mais exibido na tabela.

Configurar uma UNI para conectar dispositivos CPE a serviços de rede

As UNIs são mapeadas para portas OpenFlow e usadas para conectar um dispositivo CPE a serviços de rede. Uma UNI não pode ser mapeada para uma porta OpenFlow que já esteja mapeada para uma interface SD-WAN do tipo WAN.

Os modelos de UNI são usados para a configuração centralizada de UNIs em dispositivos CPE. Para evitar a criação de uma UNI em cada dispositivo CPE, crie uma UNI em um modelo de UNI e, em seguida, aplicar o modelo de UNI aos dispositivos CPE ao adicioná-los ou registrá-los manualmente. Ao editar uma UNI em um modelo de UNI, ela é automaticamente modificada em todos os dispositivos CPE que estiverem usando o modelo.

Ao criar uma UNI, uma interface de serviço é criada automaticamente para ela.

Gerenciar modelos de UNI

É possível visualizar a tabela de modelos de UNI na seção **SD-WAN** →**Modelos de UNI**. As informações sobre modelos de UNI são exibidas nas seguintes colunas da tabela:

- **ID** é o ID do modelo de UNI.
- **Nome** é o nome do modelo de UNI.
- **Usado** indica se o modelo de UNI está sendo usado por dispositivos CPE:
  - **Sim**.
  - **Não**.
- **Atualizado** é a data e hora em que as configurações do modelo de UNI foram modificadas pela última vez.
- **Usuário** é o nome do usuário que criou o modelo de UNI.
- **Proprietário** é o locatário ao qual o modelo de UNI pertence.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

É possível gerenciar as configurações de modelos de UNI nas seguintes guias:

- **Informações** são as informações básicas sobre o modelo de UNI. É possível editar o nome do modelo de UNI no campo **Nome**.
- **UNIs** contém UNIs que foram criadas no modelo de UNI.

Criar um modelo de UNI

Para criar um modelo de UNI:

1. No menu, acesse vá para a subseção **SD-WAN → Modelos de UNI**.

   Uma tabela de modelos de UNI é exibida.

2. Na parte superior da página, clique em **+ Modelo de UNI**.
3. Na janela aberta, insira o nome do modelo de UNI.
4. Clique em **Criar**.

O modelo de UNI é criado e exibido na tabela.

É necessário configurar o modelo de UNI criado. Para obter detalhes sobre o gerenciamento de modelos de UNI, consulte Gerenciar modelos de UNI.

Excluir um modelo de UNI

Os modelos de UNI excluídos não podem ser restaurados.

Para excluir um modelo de UNI:

1. No menu, acesse vá para a subseção **SD-WAN → Modelos de UNI**.

   Uma tabela de modelos de UNI é exibida.

2. Clique no modelo de UNI que deseja excluir.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de UNI e o locatário ao qual o modelo de UNI está atribuído.

3. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.
4. Na janela de confirmação, clique em **Excluir**.

O modelo de UNI é excluído e não é mais exibido na tabela.

Gerenciar UNIs

Gerenciar UNIs em um modelo de UNI

Para visualizar a tabela de UNIs em um modelo de UNI, vá para a seção **SD-WAN** → **Modelos de UNI** do menu, clique no modelo de UNI e selecione a guia **UNIs**. As informações sobre UNIs são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da UNI.
- **Porta OpenFlow** é o número da porta OpenFlow mapeada para a UNI.
- **Classificação** é o tipo de classificação de tráfego na UNI:
  - **Acesso**
  - **VLAN**
  - **Q-in-Q**
- **Ações** contém as ações que podem ser executadas com a UNI.

Gerenciar UNIs em um dispositivo CPE

Para visualizar a lista de UNIs em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **UNIs**.

Criar uma UNI

É possível criar uma UNI em um modelo de UNI ou dispositivo CPE. UNIs criadas no modelo de UNI são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma UNI:

1. Crie uma UNI de uma das seguintes formas:
   - Para criar uma UNI em um modelo de UNI, vá para a seção **SD-WAN** → **Modelos de UNI** do menu, clique no modelo de UNI e selecione a guia **UNIs**.
   - Para criar uma UNI em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **UNIs**.

   Uma tabela ou lista de UNIs é exibida.
2. Clique em **+ UNI**.
3. Na janela aberta, no campo **Nome**, insira o nome da UNI.

4. Especifique a porta OpenFlow para a qual a UNI é mapeada de uma das seguintes formas:

   - Se estiver criando uma UNI em um modelo de UNI, insira o número da porta OpenFlow no campo**Porta OpenFlow**.
   - Se estiver criando uma UNI em um dispositivo CPE, selecione a porta OpenFlow na lista suspensa **Porta**.

5. Na lista suspensa **Classificação**, selecione o tipo de classificação de tráfego na UNI:

   - **Acesso** Esse é o nível padrão.
   - **VLAN** Ao selecionar essa opção, no campo **ID da VLAN**, insira a tag VLAN externa da UNI. Intervalo de valores: 1 a 4094.
   - **Q-in-Q**: ao selecionar essa opção, faça o seguinte:

     a. No campo **ID da VLAN**, insira a tag VLAN externa da UNI. Intervalo de valores: 1 a 4094.

     b. No campo **ID da VLAN interna**, insira a tag VLAN interna da UNI. Intervalo de valores: 1 a 4094.

6. Se estiver criando uma UNI em um dispositivo CPE, na lista suspensa **QoS**, selecione uma regra de qualidade de serviço criada para a UNI.

7. Clique em **Criar**.

   A UNI é criada e exibida na tabela ou lista.

8. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de UNI ou dispositivo CPE.

Visualizar a utilização da UNI

Se necessário, é possível verificar quais serviços de rede estão usando a UNI em um dispositivo CPE. Por exemplo, se um modelo de UNI estiver em uso, ele não pode ser excluído.

Para ver se um modelo de UNI está sendo usado:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja visualizar o uso da UNI.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **UNIs**.

   Uma lista de UNIs é exibida.

4. Clique em **Gerenciamento → Mostrar utilização** ao lado da UNI cujo uso deseja visualizar.

Isso abre uma janela com uma tabela de serviços de rede que estão usando a UNI.

Editar uma UNI

É possível editar uma UNI em um modelo de UNI. Uma UNI editada no modelo de UNI é editada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma UNI:

1. No menu, acesse vá para a subseção **SD-WAN → Modelos de UNI**.

   Uma tabela de modelos de UNI é exibida.

2. Clique no modelo de UNI no qual deseja editar uma UNI.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de UNI e o locatário ao qual o modelo de UNI está atribuído.

3. Selecione a guia **UNI**.

   Uma tabela de UNIs é exibida.

4. Clique em **Editar** ao lado da UNI que deseja editar.

5. Na janela aberta, se necessário, edite as configurações da UNI. Para obter uma descrição das configurações, consulte as instruções para criar uma UNI.

6. Clique em **Salvar**.

   A UNI é modificada e atualizada na tabela.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de UNI.

Excluir uma UNI

É possível excluir uma UNI em um modelo de UNI ou dispositivo CPE. Uma UNI excluída no modelo de UNI é excluída automaticamente em todos os dispositivos CPE que usam o modelo.

UNIs excluídas não podem ser restauradas.

Excluir uma UNI em um modelo de UNI

Para excluir uma UNI em um modelo de UNI:

1. No menu, acesse vá para a subseção **SD-WAN → Modelos de UNI**.

   Uma tabela de modelos de UNI é exibida.

2. Clique no modelo de UNI do qual deseja excluir uma UNI.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de UNI e o locatário ao qual o modelo de UNI está atribuído.

3. Selecione a guia **UNIs**.

   Uma tabela de UNIs é exibida.

4. Clique em **Excluir** ao lado da UNI que deseja excluir.

   A UNI é excluída e não é mais exibida na tabela.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de UNI.

Excluir uma UNI em um dispositivo CPE

Não é possível excluir uma UNI se ela estiver sendo usada por pelo menos um serviço de rede. Para remover uma UNI sendo usada por serviços de rede, primeiro remova a UNI da topologia de serviços de rede. É possível verificar que serviços de rede estão usando a UNI.

Para excluir uma UNI em um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE do qual deseja excluir uma UNI.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **UNIs**.

   Uma lista de UNIs é exibida.

4. Clique em **Gerenciamento** → **Excluir** ao lado da UNI que deseja excluir.

5. Na janela de confirmação, clique em **Excluir**.

   A UNI é excluída e não é mais exibida na tabela.

6. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

Adicionar uma rota estática

Além da troca de rotas dinâmicas entre dispositivos CPE e dispositivos de rede externos pelos protocolos BGP e OSPF, o Kaspersky SD-WAN é compatível com rotas IPv4 estáticas. É possível adicionar uma rota estática em um modelo de CPE ou em um dispositivo CPE. Uma rota estática adicionada ao modelo de CPE é automaticamente adicionada a todos os dispositivos CPE que usam o modelo.

Para adicionar uma rota estática:

1. Adicione uma rota estática de uma das seguintes formas:

   - Para adicionar uma rota estática em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Rotas estáticas**.
   - Para adicionar uma rota estática em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Rotas estáticas** e marque a caixa de seleção **Substituir**.

   Uma tabela de rotas estáticas é exibida.

2. Clique em **+ Adicionar**.
3. Na lista suspensa **VRF**, selecione uma tabela de roteamento e encaminhamento virtual. Essa é uma configuração obrigatória.
4. Na lista suspensa **Interface**, selecione a interface de rede de origem da rota estática criada. Essa é uma configuração obrigatória se VRF main/254 for selecionado como tabela de roteamento e encaminhamento virtual.

   A lista de interfaces que podem ser selecionadas depende do VRF selecionado na etapa anterior. É possível selecionar apenas as interfaces que pertencem ao VRF selecionado, exceto main/254, e quaisquer interfaces do VRF main/254.
5. No campo **Destino**, insira o endereço IPv4 de destino da rota estática.
6. Se necessário, no campo **Netmask IPv4**, insira o endereço IPv4 da sub-rede de destino da rota estática.
7. No campo **Gateway**, insira o endereço IPv4 do gateway da rota estática.

   Não é possível especificar um valor nesse campo se o tipo de rota **blackhole** for selecionado na lista **Tipo**.
8. No campo **Métrica**, insira uma métrica para a rota estática. O valor padrão é `0`.

   Não é possível especificar um valor nesse campo se o tipo de rota **blackhole** for selecionado na lista **Tipo** ou se a rota estática estiver sendo criada em uma tabela de roteamento e encaminhamento virtual diferente de VRF main/254.
9. No campo **MTU**, insira o valor de MTU para a rota estática.

   Não é possível especificar um valor nesse campo se o tipo de rota **blackhole** for selecionado na lista **Tipo** ou se a rota estática estiver sendo criada em uma tabela de roteamento e encaminhamento virtual diferente de VRF main/254.
10. No campo **AD**, insira a distância administrativa para a rota estática.

    Não é possível especificar um valor nesse campo se a rota estática estiver sendo criada no VRF main/254. O valor padrão é `1`.

    Para ver a tabela de correspondência entre distâncias administrativas e protocolos de roteamento, consulte o artigo relevante.
11. Na lista suspensa **Tipo**, selecione o tipo da rota estática:

    - **unicast**. Essa é a configuração padrão.
    - **local** Apenas para VRF main/254.
    - **broadcast** Apenas para VRF main/254.

- **multicast** Apenas para VRF main/254.
- **unreachable** Apenas para VRF main/254.
- **prohibit** Apenas para VRF main/254.
- **anycast** Apenas para VRF main/254.
- **blackhole**

  Ao selecionar o tipo de rota **blackhole**, os campos **Gateway**, **Métrica** e **MTU** são desativados.

  > Para usar a rota blackhole padrão, 0.0.0.0/0, para isolar rotas entre VRFs, adicione-a ao VRF relevante na guia **VRF** na seção **SD-WAN→ Modelos de CPE**ou **SD-WAN→ CPE** selecionando **Adicionar rota blackhole**. Ao tentar adicionar essa rota na guia **Rotas estáticas**, uma mensagem de erro é exibida.

A rota estática é adicionada e exibida na tabela. É possível adicionar várias rotas estáticas ou excluir rotas estáticas. Para excluir uma rota estática, clique no ícone de exclusão ✕ ao lado dela.

12. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Tabela de correspondência de distâncias administrativas e protocolos de roteamento

Protocolo	Distância
Sistema	0
Kernel	0
Connect	0
Estática	1
NHRP	10
EBGP	20
EIGRP	90
BABEL	100
OSPF	110
ISIS	115
OPENFABRIC	115
RIP	120
Tabela	150
SHARP	150
IBGP	200
PBR	200

Filtrar rotas e pacotes de tráfego

É possível usar os seguintes mecanismos para filtrar rotas ao trabalhar com os protocolos BGP e OSPF, bem como para filtrar pacotes de tráfego ao trabalhar com o protocolo PIM:

- As listas de controle de acesso (ACL) permitem ou recusam os prefixos IPv4 especificados.
- As listas de prefixos são uma versão estendida das listas de controle de acesso. Além disso, elas permitem ou bloqueiam prefixos IPv4 no intervalo de comprimento de prefixo especificado. É possível usar listas de prefixos em mapas de roteamento.
- As Listas de comunidades permitem gerenciar prefixos com base em marcações. É possível usar listas de comunidades em mapas de roteamento.
- Mapas de roteamento são uma versão estendida das listas de prefixos. Os mapas de roteamento também modificam os valores de atributos.

É possível criar regras em listas de controle de acesso, listas de prefixos, listas de comunidades e mapas de roteamento. Cada regra é numerada. A regra com o menor número sequencial é a primeira a ser aplicada a um prefixo IPv4. Se nenhuma das regras puder ser aplicada, o prefixo IPv4 é negado.

Os mecanismos de filtragem descritos abaixo podem ser usados em diferentes cenários de roteamento, como os seguintes:

- Para distribuir o tráfego entre links e simplificar o balanceamento de carga e as políticas de failover
- Para enviar o tráfego de diferentes sub-redes (ou aplicativos) para um link definido antecipadamente
- Para rotear o tráfego para determinados serviços corporativos (por exemplo, data centers) por meio de um link mais rápido/mais caro e o restante do tráfego por meio de um link mais barato
- Para tornar um dos links menos atraente para provedores externos, adicionando um caminho AS mais longo às suas rotas

Gerenciar listas de controle de acesso (ACLs)

É possível visualizar a tabela de listas de controle de acesso em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de listas de controle de acesso em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Listas de controle de acesso**.
- Para visualizar a tabela de listas de controle de acesso em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Filtros de roteamento → Listas de controle de acesso**.

As informações sobre listas de controle de acesso são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da lista de controle de acesso.
- **Herdado** indica se a lista de controle de acesso é herdada do modelo de CPE:
  - **Sim**.
  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.
- **Sequência** é o número de sequência da regra na lista de controle de acesso. A regra com o menor número sequencial é a primeira a ser aplicada ao prefixo IPv4 pela lista de controle de acesso.
- **Rede** é o prefixo IPv4 ao qual a lista de controle de acesso aplica a regra.
- **Ação** é a ação que a regra executa no prefixo IPv4:
  - **Permitir** permite o prefixo IPv4.
  - **Negar** bloqueia o prefixo IPv4.
- **Gerenciamento** contém as ações que podem ser executadas na lista de controle de acesso.

Criar uma lista de controle de acesso

É possível criar uma lista de controle de acesso em um modelo de CPE ou dispositivo CPE. Listas de controle de acesso criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma lista de controle de acesso:

1. Crie uma lista de controle de acesso de uma das seguintes formas:
   - Para criar uma lista de controle de acesso em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Listas de controle de acesso**.
   - Para criar uma lista de controle de acesso em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Filtros de roteamento → Listas de controle de acesso** e marque a caixa de seleção **Substituir**.

   Uma tabela de listas de controle de acesso é exibida.
2. Clique em **+ Lista de controle de acesso**.
3. Na janela aberta, no campo **Nome**, insira o nome da lista de controle de acesso. O comprimento máximo do nome é de 50 caracteres. Não use espaços nesse campo.

4. Crie uma regra na lista de controle de acesso:

   a. Clique em **+ Regra**.

   b. No campo **Sequência**, insira o número sequencial da regra. A regra com o menor número sequencial é a primeira a ser aplicada ao prefixo IPv4 pela lista de controle de acesso. Intervalo de valores: 1 a 4.294.967.295.

   c. Na lista suspensa **Rede**, selecione o tipo da regra:

   - **Qualquer rede** para uma regra que permite ou nega todos os prefixos IPv4.
   - **Endereço/máscara IP**para uma regra que permite ou nega o prefixo IPv4 especificado. Essa é a configuração padrão. Ao selecionar esse valor, insira o prefixo IPv4 no campo exibido.

   d. Na lista suspensa **Ação**, selecione a ação que a regra executa com o prefixo IPv4:

   - **Permitir** permite o prefixo IPv4. Essa é a configuração padrão.
   - **Negar** bloqueia o prefixo IPv4.

   A regra é criada. É possível criar várias regras ou excluir regras. Para excluir uma regra, clique no ícone de exclusão ✕ ao lado dela.

5. Clique em **Criar**.

   A lista de controle de acesso é criada e exibida na tabela.

6. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma lista de controle de acesso

É possível editar uma lista de controle de acesso em um modelo de CPE ou dispositivo CPE. Uma lista de controle de acesso editada no modelo de CPE é editada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma lista de controle de acesso:

1. Edite uma lista de controle de acesso de uma das seguintes formas:

   - Para editar uma lista de controle de acesso em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Listas de controle de acesso**.
   - Para editar uma lista de controle de acesso em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Filtros de roteamento → Listas de controle de acesso** e marque a caixa de seleção **Substituir**.

   Uma tabela de listas de controle de acesso é exibida.

2. Clique em **Editar** ao lado da lista de controle de acesso que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da lista de controle de acesso. Para obter uma descrição das configurações, consulte as instruções para criar uma lista de controle de acesso.

4. Clique em **Salvar**.

   A lista de controle de acesso é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma lista de controle de acesso

É possível excluir uma lista de controle de acesso em um modelo de CPE ou dispositivo CPE. Uma lista de controle de acesso excluída no modelo de CPE é excluída automaticamente em todos os dispositivos CPE que usam o modelo.

As listas de controle de acesso excluídas não podem ser restauradas.

Para excluir uma lista de controle de acesso:

1. Exclua uma lista de controle de acesso de uma das seguintes formas:

   - Para excluir uma lista de controle de acesso em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Listas de controle de acesso**.

   - Para excluir uma lista de controle de acesso em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Filtros de roteamento → Listas de controle de acesso** e marque a caixa de seleção **Substituir**.

   Uma tabela de listas de controle de acesso é exibida.

2. Clique em **Excluir** ao lado da lista de controle de acesso que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A lista de controle de acesso é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar listas de prefixos

É possível visualizar a tabela de listas de prefixos em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de listas de prefixos em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Listas de prefixos**.

- Para visualizar a tabela de listas de prefixos em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Filtros de roteamento → Listas de prefixos**.

As informações sobre listas de prefixos são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da lista de prefixos.
- **Herdado** indica se a lista de prefixos é herdada do modelo de CPE:
  - **Sim**.
  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.
- **Sequência** é o número de sequência da regra na lista de prefixos. A regra com o menor número sequencial é a primeira a ser aplicada ao prefixo IPv4 pela lista de prefixos.
- **Rede** é o prefixo IPv4 ao qual a lista de prefixos aplica a regra.
- **Ação** é a ação que a regra executa no prefixo IPv4:
  - **Permitir** permite o prefixo IPv4.
  - **Negar** bloqueia o prefixo IPv4.
- **Maior ou igual** é o valor inicial do intervalo de comprimento de prefixo ao qual a lista de prefixos aplica a regra.
- **Menor ou igual** é o valor final do intervalo de comprimento de prefixo ao qual a lista de prefixos aplica a regra.
- **Gerenciamento** contém as ações que podem ser executadas na lista de prefixos.

Criar uma lista de prefixos

É possível criar uma lista de prefixos em um modelo de CPE ou dispositivo CPE. Listas de prefixos criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma lista de prefixos:

1. Crie uma lista de prefixos de uma das seguintes formas:
   - Para criar uma lista de prefixos em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Listas de prefixos**.
   - Para criar uma lista de prefixos em um dispositivo CPE, vá para a seção **SD-WAN** do menu, clique no dispositivo CPE, selecione a guia **Filtros de roteamento → Listas de prefixos** e marque a caixa de seleção **Substituir**.

   Uma tabela de listas de prefixos é exibida.
2. Clique em **+ Lista de prefixos**.
3. Na janela aberta, no campo **Nome**, insira o nome da lista de prefixos. O comprimento máximo do nome é de 50 caracteres. Não use espaços nesse campo.

4. Criar uma regra na lista de prefixos:

   a. Clique em **+ Regra**.

   b. No campo **Sequência**, insira o número sequencial da regra. A regra com o menor número sequencial é a primeira a ser aplicada ao prefixo IPv4 pela lista de prefixos. Intervalo de valores: 1 a 4.294.967.295.

   c. Na lista suspensa **Rede**, selecione o tipo da regra:

   - **Qualquer rede** para uma regra que permite ou nega todos os prefixos IPv4.
   - **Endereço/máscara IP**para uma regra que permite ou nega o prefixo IPv4 especificado. Essa é a configuração padrão. Ao selecionar esse valor, insira o prefixo IPv4 no campo exibido.

   d. Na lista suspensa **Ação**, selecione a ação que a regra executa com o prefixo IPv4:

   - **Permitir** permite o prefixo IPv4. Essa é a configuração padrão.
   - **Negar** bloqueia o prefixo IPv4.

   e. No campo **Maior ou igual**, insira o valor inicial do intervalo de comprimento de prefixo ao qual a lista de prefixos aplica a regra. Intervalo de valores: 0 a 32.

   f. No campo **Menor ou igual**, insira o valor final do intervalo de comprimento de prefixo ao qual a lista de prefixos aplica a regra. Intervalo de valores: 0 a 32.

   A regra é criada. É possível criar várias regras ou excluir regras. Para excluir uma regra, clique no ícone de exclusão ✕ ao lado dela.

5. Clique em **Criar**.

   A lista de prefixos é criada e exibida na tabela.

6. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma lista de prefixos

É possível editar uma lista de prefixos em um modelo de CPE ou dispositivo CPE. Uma lista de prefixos editada no modelo de CPE é editada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma lista de prefixos:

1. Edite uma lista de prefixos de uma das seguintes formas:

   - Para editar uma lista de prefixos em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Listas de prefixos**.
   - Para editar uma lista de prefixos em um dispositivo CPE, vá para a seção **SD-WAN** do menu, clique no dispositivo CPE, selecione a guia **Filtros de roteamento → Listas de prefixos** e marque a caixa de seleção **Substituir**.

   Uma tabela de listas de prefixos é exibida.

2. Clique em **Editar** ao lado da lista de prefixos que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da lista de prefixos. Para obter uma descrição das configurações, consulte as instruções para criar uma lista de prefixos.

4. Clique em **Salvar**.

   A lista de prefixos é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma lista de prefixos

É possível excluir uma lista de prefixos em um modelo de CPE ou dispositivo CPE. Uma lista de prefixos excluída do modelo de CPE é excluída automaticamente de todos os dispositivos CPE que usam o modelo.

As listas de prefixos excluídas não podem ser restauradas.

Para excluir uma lista de prefixos:

1. Exclua uma lista de prefixos de uma das seguintes formas:

   - Para excluir uma lista de prefixos em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Listas de prefixos**.

   - Para excluir uma lista de prefixos em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Filtros de roteamento → Listas de prefixos** e marque a caixa de seleção **Substituir**.

   Uma tabela de listas de prefixos é exibida.

2. Clique em **Excluir** ao lado da lista de prefixos que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A lista de prefixos é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar listas de comunidades

É possível visualizar a tabela de listas de comunidades em um modelo de CPE e em um dispositivo CPE:

Para visualizar a tabela de listas de comunidades em um modelo de CPE, acesse a seção SD-WAN → Modelos de CPE do menu, clique no modelo de CPE e selecione a guia Roteamento → Filtros de roteamento → Listas de comunidades.

Para visualizar a tabela de listas de comunidades em um dispositivo CPE, acesse a seção SD-WAN → CPEs do menu, clique no dispositivo CPE e selecione a guia Roteamento → Filtros de roteamento → Listas de comunidades.

As informações sobre listas de comunidades são exibidas nas seguintes colunas da tabela:

"Nome" é o nome da lista de comunidades

Substituir:

"Sim" significa que as configurações das listas de comunidades são exclusivas e não herdadas de um modelo.

"Não" significa que as configurações da lista de comunidades são herdadas do modelo.

Essa coluna é exibida apenas no dispositivo CPE. É possível alterar o valor nessa coluna para cada lista de comunidades diretamente na tabela.

"Herdado" indica se a lista de comunidades é herdada do modelo de CPE:

Sim

Não

Essa coluna também é exibida apenas no dispositivo CPE.

"Tipo" é o tipo da lista de comunidades: padrão ou avançado.

"Sequência" é o número de sequência da regra na lista de comunidades. A lista de comunidades aplica a regra começando pelo número mais baixo.

"Ação" é a ação que a regra executa com o valor 'community':

"Permitir" permite a comunidade

"Recusar" recusa a comunidade

"Valor" marca o prefixo IPv4, permitindo que políticas sejam aplicadas a ele.

Criar uma lista de comunidades

É possível criar uma lista de comunidades em um modelo de CPE ou dispositivo CPE.

Crie uma lista de comunidades de uma das seguintes formas:

Se você quiser criar uma lista de comunidades em um modelo de CPE, acesse a seção SD-WAN → Modelos de CPE → Roteamento → Filtros de roteamento → Listas de comunidades e, na parte superior da página, clique no botão "+ Adicionar".

Se você quiser criar uma lista de comunidades em um dispositivo CPE, acesse a seção SD-WAN → CPEs, selecione a guia Roteamento → Filtros de roteamento → Listas de comunidades e, na parte superior da página, clique no botão "+ Adicionar".

Uma tabela de listas de comunidades é exibida.

Na janela exibida, no campo "Nome", insira o nome da lista de comunidades. O comprimento máximo do nome é de 50 caracteres.

Observe que o nome da lista de comunidades deve ser exclusivo em uma locação.

No campo "Tipo", selecione o tipo de comunidade padrão (correspondência estrita de valor) ou avançado (correspondência de expressão regular).

Agora, você pode clicar em "+ Adicionar" para adicionar registros de comunidade à lista.

O campo "Ordem dos registros de comunidade" gera automaticamente números em incrementos de 10, começando em 10. Você pode alterar o número de sequência (e a ordem na qual os registros são aplicados) usando o item de menu "Contador".

Em seguida, selecione uma "Ação" para o registro de comunidade: "Recusar" ou "Permitir".

Tipo de comunidade padrão

Em seguida, você pode inserir os valores de comunidade selecionando-os na lista suspensa ou inserindo-os como uma lista de valores de texto. Uma comunidade também pode ser especificada como um valor numérico no formato <número de 0 a 65535>:<número de 0 a 65535>. Combinações de valores personalizados e valores predefinidos são possíveis.

Tipo de comunidade avançado

Em seguida, você pode inserir valores de comunidade como uma expressão regular.

Se você quiser remover um registro de comunidade da lista, marque a caixa de seleção correspondente e clique no botão "Excluir".

Agora, a lista de comunidades criada pode ser usada nas instruções 'match' e/ou 'set' dentro do mapa de roteamento para manipular prefixos BGP (link para a seção "Gerenciar mapas de roteamento").

Editar uma lista de comunidades

Para editar uma lista de comunidades, marque sua caixa de seleção e clique no botão "Editar" ou no nome da lista de comunidades.

Agora você pode adicionar ou excluir registros da lista de comunidades.

Excluir uma lista de comunidades

Para excluir uma lista de comunidades, marque sua caixa de seleção e clique no botão "Excluir". Somente é possível excluir uma lista por vez.

Criar uma lista de comunidades

É possível criar uma lista de comunidades em um modelo de CPE ou dispositivo CPE. As listas de comunidades criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma lista de comunidade:

1. Crie uma lista de comunidades de uma das seguintes formas:

   - Para criar uma lista de comunidades em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Roteamento → Filtros de roteamento → Listas da comunidade**.

   - Para criar uma lista de comunidades em um dispositivo CPE, vá para a seção **SD-WAN** do menu, clique no dispositivo CPE e selecione a guia **Roteamento → Filtros de roteamento → Listas da comunidade**.

   Uma tabela de listas de comunidades é exibida.

2. Clique em **+ Adicionar**.

3. Isso abre uma janela; na janela aberta, no campo **Nome**, insira o nome da lista de comunidades. O comprimento máximo do nome é de 50 caracteres. Não use espaços nesse campo.

   O nome da lista de comunidades deve ser exclusivo na locação.

4. Na lista suspensa **Tipo**, selecione o tipo da lista de comunidades:

   - **Standard**

     As rotas são correspondidas com base em correspondências exatas dos valores dos atributos da comunidade.

   - **Extended**

     As rotas são correspondidas com base em expressões regulares.

5. Criar uma regra na lista de comunidades:

   a. Clique em **+ Adicionar**.

   b. No campo **Sequência**, insira o número sequencial da regra. A regra com o menor número sequencial é a primeira a ser aplicada ao prefixo IPv4 pela lista de comunidades. Intervalo de valores: 1 a 4.294.967.295.

   c. Na lista suspensa **Ação**, selecione a ação que a regra executa no prefixo IPv4:

      - **Permitir** permite o prefixo IPv4. Essa é a configuração padrão.

      - **Negar** bloqueia o prefixo IPv4.

   d. Especifique o critério de filtragem que a regra aplica às rotas:

      - Para listas de comunidade padrão, na coluna Comunidade, especifique um ou mais atributos da comunidade selecionando valores predefinidos na lista suspensa ou inserindo manualmente valores de texto ou valores no formato <número de 0 a 65535>:<número de 0 a 65535>. Você pode combinar valores inseridos manualmente e valores predefinidos.

        Os seguintes valores predefinidos estão disponíveis:

        - `local-AS`

        - `no-advertise`

- `no-export`
- `internet`
- `graceful-shutdown`
- `accept-own-nexthop`
- `accept-own`
- `route-filter-translated-v4`
- `route-filter-v4`
- `route-filter-translated-v6`
- `route-filter-v6`
- `llgr-stale`
- `no-llgr`
- `blackhole`
- `no-peer`

- Para listas de comunidades estendidas, no campo na coluna **Expressão regular**, insira uma expressão regular BGP para especificar os limites dos números AS. A sintaxe de expressões regulares BGP é um subconjunto da sintaxe de expressões regulares POSIX e usa o caractere especial de sublinhado '_' para representar espaços, vírgulas, delimitadores de conjunto AS { }, delimitadores de confederação AS ( ) e o início e o fim de uma linha.

A regra é criada. É possível criar várias regras ou excluir regras. Para excluir uma regra, clique no ícone de exclusão ao lado dela.

6. Clique em **Criar**.

   A lista de comunidades é criada e exibida na tabela.

   Você pode usar a lista de comunidades gerada nos mapas de roteamento para fazer a correspondência por prefixo ou para alterar os atributos de prefixo.

7. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma lista de comunidades

É possível editar uma lista de comunidades em um modelo de CPE ou dispositivo CPE. As listas de comunidades editadas no modelo de CPE são automaticamente modificadas em todos os dispositivos CPE que usam o modelo.

Para editar uma lista de comunidades:

1. Edite uma lista de comunidades de uma das seguintes formas:

   - Para editar uma lista de comunidades em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Roteamento → Filtros de roteamento → Listas da comunidade**.

   - Para editar uma lista de comunidades em um dispositivo CPE, vá para a seção **SD-WAN** do menu, clique no dispositivo CPE e selecione a guia **Roteamento → Filtros de roteamento → Listas da comunidade**.

   Uma tabela de listas de comunidades é exibida.

2. Clique no nome da lista de comunidades que deseja editar ou selecione-a na tabela e clique no botão **Editar**.

3. Uma janela será aberta para você editar as configurações da lista de comunidades, caso necessário. Para obter uma descrição das configurações, consulte as instruções para criar uma lista de comunidades.

4. Clique em **Salvar**.

   A lista de comunidades é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma lista de comunidades

É possível excluir listas de comunidades em um modelo de CPE ou dispositivo CPE. As listas de comunidades excluídas no modelo de CPE são automaticamente excluídas em todos os dispositivos CPE que usam o modelo.

As listas de comunidades excluídas não podem ser restauradas.

Para excluir uma lista de comunidades:

1. Exclua uma lista de comunidades de uma das seguintes formas:

   - Para excluir uma lista de comunidades em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Roteamento → Filtros de roteamento → Listas da comunidade**.

   - Para excluir uma lista de comunidades em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Roteamento → Filtros de roteamento → Listas da comunidade**.

   Uma tabela de listas de comunidades é exibida.

2. Na tabela, selecione a lista de comunidades que deseja excluir e clique no botão**Excluir**.

3. Na janela de confirmação, clique em **Excluir**.

   A lista de comunidades é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar mapas de roteamento

É possível visualizar a tabela de mapas de roteamento em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de mapas de roteamento em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento** → **Mapas de roteamento**.
- Para visualizar a tabela de mapas de roteamento em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **Filtros de roteamento** → **Mapas de roteamento**.

As informações sobre mapas de roteamento são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do mapa de roteamento.
- **Herdado** indica se o mapa de roteamento é herdado do modelo de CPE:
  - **Sim**.
  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.
- **Sequência** é o número de sequência da regra no mapa de roteamento. A regra com o menor número sequencial é a primeira a ser aplicada ao prefixo IPv4 pelo mapa de roteamento.
- **Ação** é a ação que a regra executa no prefixo IPv4:
  - **Permitir** permite o prefixo IPv4.
  - **Negar** bloqueia o prefixo IPv4.
- **Tipo de correspondência** é o critério que faz com que o mapa de roteamento aplique a regra ao prefixo IPv4:
  - **Nenhum** aplica a regra a todos os prefixos IPv4.
  - **Prefix-List** aplica a regra aos prefixos IPv4 permitidos pela lista de prefixos especificada.
  - A **lista de comunidades** aplica a regra aos prefixos IPv4 permitidos pela lista de comunidades especificada.
- **Valor** é um prefixo IPv4 que a lista de prefixos deve permitir para que o mapa de roteamento aplique a regra ao prefixo IPv4. Essa coluna só exibe um valor se a coluna **Tipo de correspondência** exibir **Prefix-List**.
- **Alterar atributo** é o atributo cujo valor altera a regra.

- **Novo valor** é o valor que a regra define para o atributo.
- **Gerenciamento** contém as ações que podem ser executadas com o mapa de roteamento.

Criar um mapa de roteamento

É possível criar um mapa de roteamento em um modelo de CPE ou dispositivo CPE. Mapas de roteamento criados no modelo de CPE são criados automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar um mapa de roteamento:

1. Crie um mapa de roteamento de uma das seguintes formas:
   - Para criar um mapa de roteamento em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Mapas de roteamento**.
   - Para criar um mapa de roteamento em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Filtros de roteamento → Mapas de roteamento** e marque a caixa de seleção **Substituir**.

   Uma tabela de mapas de roteamento é exibida.
2. Clique em **+ Mapa de roteamento**.
3. Na janela aberta, no campo **Nome**, insira o nome do mapa de roteamento. O comprimento máximo do nome é de 50 caracteres. Não use espaços nesse campo.
4. Criar uma regra no mapa de roteamento:
   a. Clique em **+ Regra**.
   b. No campo **Sequência**, insira o número sequencial da regra. A regra com o menor número sequencial é a primeira a ser aplicada ao prefixo IPv4 pelo mapa de roteamento. Intervalo de valores: 1 a 4.294.967.295.
   c. Na lista suspensa **Ação**, selecione a ação que a regra executa no prefixo IPv4:
      - **Permitir** permite o prefixo IPv4. Essa é a configuração padrão.
      - **Negar** bloqueia o prefixo IPv4.
   d. Na lista suspensa **Tipo de correspondência**, selecione o critério que faz com que o mapa de roteamento aplique a regra ao prefixo IPv4:
      - **Nenhum** aplica a regra a todos os prefixos IPv4. Essa é a configuração padrão.
      - **Prefix-List** aplica a regra aos prefixos IPv4 permitidos pela lista de prefixos especificada. Ao selecionar esse valor, na lista suspensa **Lista de prefixos**, selecione uma lista de prefixos criada.
      - A **Lista de comunidades** aplica a regra aos prefixos IPv4 permitidos pela lista de prefixos especificada. Ao selecionar esse valor, selecione uma lista de comunidades criada na lista suspensa **Llista da comunidade**.

e. Na lista suspensa **Tipo de correspondência**, caso tenha selecionado a **Lista de prefixos** ou a **Lista de comunidades**, na lista suspensa **Alterar atributo**, selecione o atributo que a regra modifica://TODO

- **Nenhum** — Não alterar os valores dos atributos. Essa é a configuração padrão.
- **IP next-hop** para alterar o valor do atributo 'next-hop' para o endereço IPv4 especificado. Ao selecionar esse valor, insira um endereço IPv4 no campo **Novo valor**.
- **Local Preference** para alterar o valor do atributo 'local preference' para o valor especificado. Ao selecionar esse valor, no campo **Novo valor**, insira um valor para o atributo 'local preference'. Intervalo de valores: 0 a 4.294.967.295.
- **Metric** para alterar o valor do atributo MED para o valor especificado. Ao selecionar esse valor, no campo **Novo valor**, insira um valor para o atributo MED. Intervalo de valores: 0 a 4.294.967.295.
- **AS Path Prepend** — Adicionar o número do sistema autônomo ao atributo 'as path'. Ao selecionar esse valor, insira o número do sistema autônomo no campo **Novo valor**. É possível inserir vários números separados por espaços. Intervalo de valores: 0 a 4.294.967.295.

A regra é criada. É possível criar várias regras ou excluir regras. Para excluir uma regra, clique no ícone de exclusão ✕ ao lado dela.

5. Clique em **Criar**.

   O mapa de roteamento é criado e exibido na tabela.

6. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar um mapa de roteamento

É possível editar um mapa de roteamento em um modelo de CPE ou dispositivo CPE. Um mapa de roteamento editado no modelo de CPE é editado automaticamente em todos os dispositivos CPE que usam o modelo.

> Caso deseje que as alterações feitas em um mapa de roteamento sejam aplicadas imediatamente nos pares BGP ou grupos de pares BGP que usam o mapa de roteamento, marque a caixa de seleção **BFD** ou **Recuperação suave de entrada** ao criar ou editar o par BGP ou o grupo de pares BGP.

Para editar um mapa de roteamento:

1. Edite um mapa de roteamento de uma das seguintes formas:

   - Para editar um mapa de roteamento em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e, na área de configurações exibida, selecione a guia **Filtros de roteamento → Mapas de roteamento**.
   - Para editar um mapa de roteamento em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e, na área de configurações exibida, selecione a guia **Filtros de roteamento → Mapas de roteamento** e marque a caixa de seleção **Substituir**.

   Uma tabela de mapas de roteamento é exibida.

2. Clique em **Editar** ao lado do mapa de roteamento que deseja editar.

3. Na janela aberta, se necessário, edite as configurações do mapa de roteamento. Para obter uma descrição das configurações, consulte as instruções para criar um mapa de roteamento.

4. Clique em **Salvar**.

   O mapa de roteamento é modificado e atualizado na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir um mapa de roteamento

É possível excluir um mapa de roteamento em um modelo de CPE ou dispositivo CPE. Um mapa de roteamento excluído do modelo de CPE é excluído automaticamente de todos os dispositivos CPE que usam o modelo.

Os mapas de roteamento excluídos não podem ser restaurados.

Para excluir um mapa de roteamento:

1. Exclua um mapa de roteamento de uma das seguintes formas:

   - Para excluir um mapa de roteamento em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Filtros de roteamento → Mapas de roteamento**.

   - Para excluir um mapa de roteamento em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Filtros de roteamento → Mapas de roteamento** e marque a caixa de seleção **Substituir**.

   Uma tabela de mapas de roteamento é exibida.

2. Clique em **Excluir** ao lado do mapa de roteamento que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   O mapa de roteamento é excluído e não é mais exibido na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Roteamento baseado em política (PBR)

Além do roteamento baseado em propriedades padrão de pacotes, como o endereço IP de destino, o Kaspersky SD-WAN é compatível com o Roteamento baseado em política (PBR). Esse tipo de roteamento é baseado no uso de políticas, ou seja, conjuntos de regras de roteamento ou regras de IP, criadas pelo usuário (administrador ou administrador de locatário) e armazenadas no dispositivo. A seguir estão alguns exemplos de casos de uso para o roteamento PBR:

- Redirecionar o tráfego para redes especificadas pelo usuário para contornar o firewall em caso de problemas com ele
- Redirecionar o tráfego destinado à Internet para redes especificadas pelo usuário via SD-WAN para um gateway que atua como ponto único de acesso à Internet para todos os dispositivos CPE

É possível criar e visualizar regras de roteamento na linha de comando do dispositivo CPE usando comandos do kit de ferramentas iproute2, bem como a partir da interface gráfica do orquestrador. Esta seção descreve o gerenciamento de regras de roteamento na interface gráfica do orquestrador.

Gerenciar regras de roteamento de IP

É possível visualizar a tabela de regras de IP em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de regras de IP em um modelo de CPE, vá para a seção **SD-WAN→ Modelos de CPE** do menu, clique no modelo de CPE e, na barra lateral, selecione a seção **PBR**.
- Para visualizar a tabela de regras de IP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e, na barra lateral, selecione a seção **PBR**.

As informações sobre regras de IP são exibidas nas seguintes colunas da tabela:

- **Prioridade** é a prioridade da regra. Regras com um valor de prioridade mais baixo são aplicadas primeiro.
- **Status** é o status da regra. Valores possíveis:
  - **Ativado** significa que a regra está ativa.
  - **Desativado** significa que a regra está inativa.
- **Protocolo IP** é o protocolo IP. Os seguintes valores são possíveis:
  - TCP
  - UDP
  - ICMP
  - SCTP
  - AH

- ESP
- GRE
- IPIP

- **Interface de rede de origem** é a interface de entrada a ser correspondida. Se a interface for de loopback, a regra corresponderá apenas aos pacotes originados desse host.
- **Porta de origem** é a porta de origem.
- **Host ou rede de origem** é o host ou a rede de origem.
- **Interface de rede de destino** é a interface de saída a ser correspondida. A interface de saída está disponível apenas para pacotes originados de soquetes locais vinculados ao dispositivo.
- **Porta de destino** é a porta de destino.
- **Host ou rede de destino** é o host ou a rede de destino.
- **VRF** é o VRF no qual a pesquisa de rotas é executada.
- **Ações** lista as ações que podem ser executadas com a regra de IP (ativar, desativar, editar, excluir).

Criar uma regra de IP

É possível criar uma regra de IP em um modelo de CPE ou dispositivo CPE. Regras de IP criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma regra de IP:

1. Crie uma regra de IP de uma das seguintes formas:
   - Para criar uma regra de IP em um modelo de CPE, vá para a seção **SD-WAN→ Modelos de CPE** do menu, clique no modelo de CPE e, na barra lateral, selecione a seção **PBR**.
   - Para criar uma regra de IP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e, na barra lateral, selecione a seção **PBR**.

   Uma tabela de regras de IP é exibida.
2. Clique em **+ Regra de endereço IP**.
3. Na janela aberta, no campo **Prioridade**, insira a prioridade da regra. Regras com um valor de prioridade mais baixo são aplicadas primeiro. O valor deve ser único.
4. Na lista suspensa **Protocolo IP**, selecione o protocolo IP. Os seguintes valores são possíveis:
   - TCP
   - UDP
   - ICMP

- SCTP
- AH
- ESP
- GRE
- IPIP

5. Em **Origem** e **Destino**, especifique as configurações de origem e destino para a regra de IP, conforme necessário:
   - Selecione a origem ou o destino **Tipo**: host ou rede.
   - Dependendo do **Tipo** selecionado, no campo abaixo, especifique:
     - Endereço IP de origem ou destino, caso tenha selecionado o tipo **Host** (a legenda do campo é, então, **Endereço IP**.
     - Endereço IP de origem ou destino e a máscara, caso tenha selecionado o tipo **Rede** (a legenda do campo é, então, **Endereço/máscara IP**.
   - No campo **Porta**, especifique a porta de origem ou destino.

     É possível inserir um valor único ou um intervalo de valores de 1 a 65.535 com um hífen, por exemplo: `443`, `1024-65535`.
   - Na lista suspensa **Alias da interface de rede**, selecione a interface de origem (entrada) ou a interface de destino (saída).

     Se a interface de entrada for de loopback, a regra corresponderá apenas aos pacotes originados desse host. A interface de saída está disponível apenas para pacotes originados de soquetes locais vinculados ao dispositivo.
6. Na lista suspensa **Pesquisar VRF**, selecione o VRF para procurar rotas.

   Caso tenha selecionado main/254, em **Destino**, especifique um endereço IP de origem diferente de 0.0.0.0/0, caso contrário, a regra não poderá ser salva.
7. Clique em **Criar**.

   A regra de IP é criada e exibida na tabela.
8. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE ou do dispositivo CPE.

Editar uma regra de IP

É possível criar regras de IP em um modelo de CPE ou dispositivo CPE. As regras de IP editadas no modelo de CPE são automaticamente editadas em todos os dispositivos CPE que usam o modelo.

Para editar uma regra de IP:

1. Edite uma regra de IP de uma das seguintes formas:

   - Para editar uma regra de IP em um modelo de CPE:

     - No menu, acesse a seção **SD-WAN→Modelos de CPE**, clique no modelo de CPE e, na barra lateral, selecione a seção **PBR**.

     - Na tabela de regras de IP exibida, na coluna **Ações**, clique no botão **Editar** da regra que deseja editar.

   - Para editar uma regra de IP em um dispositivo CPE:

     - No menu, acesse a seção **SD-WAN →CPE**, clique no dispositivo CPE e, na barra lateral, selecione a seção **PBR**.

     - Na tabela de regras de IP exibida, na coluna **Ações**, clique no botão **Editar** da regra que deseja editar. Se a regra de IP tiver sido herdada de um modelo, primeiro marque a caixa de seleção **Substituir** para que a regra exiba o botão **Editar**.

2. Na janela aberta, edite as configurações da regra de IP que deseja alterar: para obter uma descrição das configurações, consulte as instruções para criar uma regra de IP.

3. Clique em **Salvar**.

   A regra de IP é modificada e atualizada na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma regra de IP

É possível excluir regras de IP em um modelo de CPE ou dispositivo CPE. As regras de IP excluídas no modelo de CPE são automaticamente excluídas em todos os dispositivos CPE que usam o modelo. Em um dispositivo CPE, é possível excluir apenas as regras de IP adicionadas diretamente no dispositivo, mas não as regras herdadas do modelo.

As regras de IP excluídas não podem ser restauradas.

Para excluir uma regra de IP:

1. Exclua uma regra de IP de uma das seguintes formas:

   - Para excluir uma regra de IP em um modelo de CPE, vá para a seção **SD-WAN→ Modelos de CPE** do menu, clique no modelo de CPE e, na barra lateral, selecione a seção **PBR**.

   - Para excluir uma regra de IP não herdada do modelo de CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e, na barra lateral, selecione a seção **PBR**.

   Uma tabela de regras de IP é exibida.

2. Clique em **Excluir** ao lado da regra de IP que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A regra de IP é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

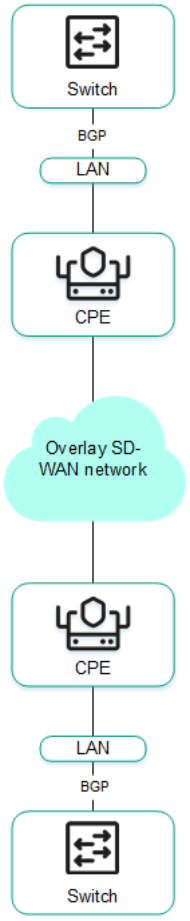
Troca de rotas por BGP

O Kaspersky SD-WAN é compatível com o protocolo de roteamento dinâmico BGP (protocolo de gateway de borda) para a troca de informações de roteamento entre dispositivos CPE e dispositivos de rede externos. É possível estabelecer sessões internas de iBGP (BGP interno), bem como sessões externas de eBGP (BGP externo).

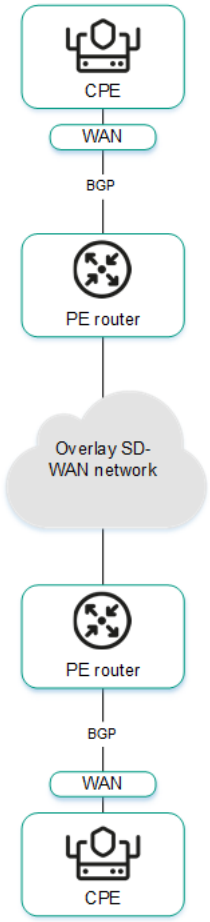
Também há suporte para a criação de pares BGP individuais e grupos de pares BGP. As sessões TCP dinâmicas são estabelecidas com grupos de pares BGP.

As figuras abaixo mostram exemplos do BGP sendo usado na solução:

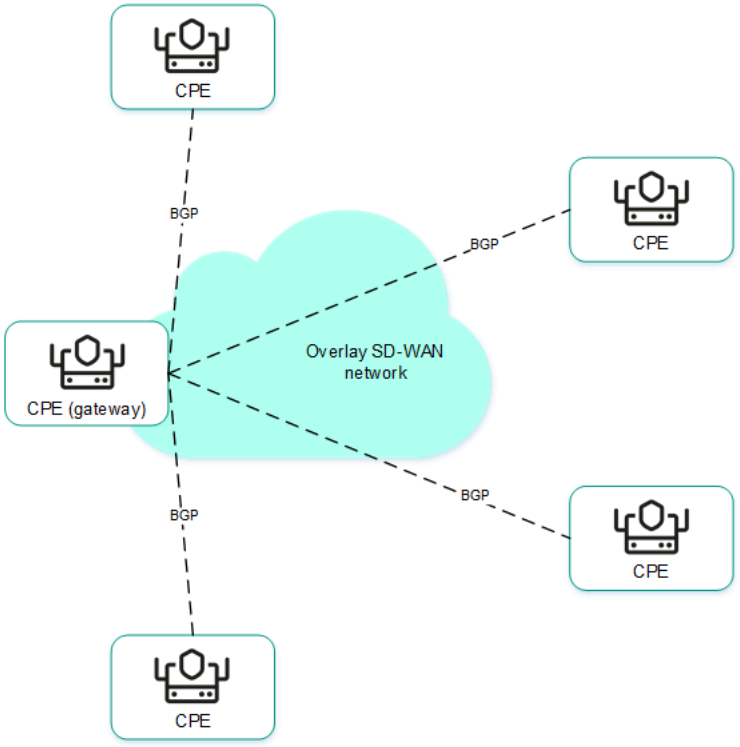
- Conectar vários locais do cliente à rede L3 SD-WAN via BGP.



- Conectar dispositivos CPE à rede IP/MPLS do provedor de serviços via BGP.



- Usar o BGP para configurar a conectividade de dispositivos CPE no domínio.



Configurações básicas de BGP

É possível especificar configurações básicas de BGP em um modelo de CPE ou dispositivo CPE. As configurações de BGP especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para modificar as configurações básicas de BGP:

1. Especifique as configurações básicas de BGP de uma das seguintes formas:

   - Para editar as configurações básicas de BGP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BGP** na barra lateral da janela exibida.

   - Para gerenciar as configurações básicas do BGP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e, na barra lateral da janela exibida, selecione a seção **BGP** e marque a caixa de seleção **Substituir**, que desbloqueia o campo **Sistema autônomo**.

2. No campo **Sistema autônomo**, insira o número do sistema autônomo (de 1 a 4.294.967.295). O sistema autônomo especificado será usado para todas as instâncias BGP criadas no dispositivo ou no modelo de CPE e será exibido no campo **AS**.

   Após especificar o número do sistema autônomo, o botão **+ BGP** fica disponível.

3. Na lista **Instância BGP padrão com VRF**, selecione a instância BGP que deve ser usada por padrão. Se nenhuma instância BGP tiver sido criada, crie uma seguindo as etapas abaixo e selecione a instância BGP criada.

4. Crie uma ou mais instâncias BGP. Para isso:

   1. Clique no botão **+ BGP**. O espaço de trabalho para adicionar uma instância BGP é exibido.

   2. Por padrão, é selecionada a guia **Configurações gerais**, que exibe as configurações básicas de BGP.

   3. Na lista suspensa **BGP**, selecione **Ativado**. O valor padrão é **Desativado**.

   4. Na lista suspensa **VRF**, selecione um VRF existente para o qual deseja anunciar rotas BGP. A lista mostra apenas os VRFs que não estão associados a outras instâncias BGP no dispositivo ou no modelo de CPE.

   5. No campo **ID do roteador**, insira o endereço IPv4 que deseja atribuir ao ID do roteador do dispositivo CPE. Para atribuir um endereço IPv4 de um intervalo de endereços IP especificado:

   6. Marque a caixa de seleção **ID do roteador do pool de IPs**. Esta caixa de seleção está desmarcada por padrão.

   7. Na lista suspensa **Pool de endereço IP**, selecione um intervalo de endereços IP criado.

   8. Se necessário, no campo **Máximo de caminhos**, insira o número máximo de entradas na tabela de roteamento e encaminhamento do dispositivo CPE. Intervalo de valores: 1 a 8.

   9. Se necessário, marque as seguintes caixas de seleção:

   10. Marque a caixa de seleção **Sempre comparar MED**. Essa caixa de seleção permite que o dispositivo CPE compare o discriminador de saída múltipla (MED) de rotas anunciadas de sistemas autônomos diferentes.

Essa caixa de seleção deve estar marcada em todos os dispositivos CPE no sistema autônomo. Caso contrário, a troca de informações de roteamento pode resultar em loops de roteamento.

- Marque a caixa de seleção **Reinicialização normal (modo auxiliar)** para ativar a reinicialização normal no dispositivo CPE.

  Essas caixas de seleção são desmarcadas por padrão.

11. Para que o dispositivo CPE não troque rotas IPv4 com pares BGP por padrão, desmarque a caixa de seleção **Usar rotas unicast IPv4 padrão**. Esta caixa de seleção é selecionada por padrão.

12. Para configurar temporizadores do BGP:

13. Marque a caixa de seleção **Temporizadores do BGP**. Esta caixa de seleção está desmarcada por padrão.

    a. No campo **Keepalive (s)**, insira o intervalo de tempo em segundos que o dispositivo CPE usa para enviar pacotes de controle aos pares BGP. Intervalo de valores: 0 a 65.535.

    b. No campo **Tempo de espera (s)**, insira o intervalo de tempo em segundos que o dispositivo CPE usa ao receber pacotes de controle de pares BGP. Se nenhum pacote de controle for recebido do par BGP dentro do tempo especificado, o dispositivo CPE considera o par indisponível. Intervalo de valores: 0 a 65.535.

14. Para configurar a redistribuição de rotas no BGP, em **Redistribuição de rotas**, faça o seguinte:

    a. Marque as caixas de seleção ao lado dos tipos de rota:

    - **Kernel** para redistribuir as rotas do Kernel geradas pelo sistema operacional do dispositivo CPE.
    - **Conectado** para redistribuir rotas diretamente conectadas às interfaces de rede do dispositivo CPE.
    - **Estática** para redistribuir rotas estáticas.
    - **OSPF** para redistribuir rotas OSPF.

    Essas caixas de seleção são desmarcadas por padrão.

    b. Na lista suspensa **Mapa de roteamento**, selecione um mapa de roteamento criado para rotas redistribuídas.

    c. No campo **Métrica**, insira uma métrica de rotas redistribuídas. Intervalo de valores: 0 a 16.777.214.

15. Para que o dispositivo CPE anuncie a sub-rede especificada aos pares BGP:

    a. Em **Redes**, clique em **+ Rede**.

    b. No campo **Rede**, insira o prefixo IPv4 da sub-rede.

    c. Na lista suspensa **Mapa de roteamento**, selecione um mapa de roteamento criado para a sub-rede.

    A sub-rede é especificada e exibida em **Redes**. É possível especificar diversas sub-redes ou excluir sub-redes. Para excluir uma sub-rede, clique no ícone de exclusão ✕ ao lado dela.

16. Se necessário, gerencie também as configurações da instância BGP nas guias **Vizinhos**, **Grupos de pares** e **Vazamento de rotas**.

17. Na parte inferior do espaço de trabalho para adição de uma instância BGP, clique em **Salvar** para salvar as configurações da instância BGP.

    A instância BGP é salva e adicionada à tabela de instâncias BGP na área de configurações.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar pares BGP

Para visualizar ou editar a tabela de pares BGP de uma instância BGP em um modelo de CPE ou em um dispositivo CPE:

1. Vá para a seção **BGP**. Para isso:

   - Para visualizar ou editar a tabela de pares BGP em um modelo de CPE, vá para a seção **SD-WAN→ Modelos de CPE** do menu, clique no modelo de CPE e, na barra lateral da área de configurações, selecione **BGP**.

   - Para visualizar ou editar a tabela de pares BGP em um dispositivo CPE, vá para a seção **SD-WAN→ CPE** do menu, clique no dispositivo CPE e, na barra lateral da área de configurações, clique em **BGP**.

2. Abra uma instância BGP existente clicando em **Editar** na linha correspondente da tabela ou crie uma nova instância BGP.

3. Na área de configurações da instância BGP, selecione a guia **Vizinhos**.

As informações sobre pares BGP são exibidas nas seguintes colunas da tabela:

- **IP do vizinho** é o endereço IPv4 do par BGP.
- **Nome** é o nome do par BGP.
- **Descrição** é uma breve descrição do par BGP.
- **Herdado** indica se o par BGP é herdado do modelo de CPE:

  - **Sim**.

  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.

- **AS remoto** é o número do sistema autônomo do par BGP.
- **Desligar** indica se o par BGP está desativado e nenhuma sessão TCP foi estabelecida com ele.

  - **Sim**.

  - **Não**.

- **Peso** é o peso das rotas anunciadas pelo par BGP.
- **Gerenciamento** contém as ações que podem ser executadas com o par BGP.

Criar um par BGP

É possível criar um par BGP em um modelo de CPE ou dispositivo CPE. Pares BGP criados no modelo de CPE são criados automaticamente em todos os dispositivos CPE que usam o modelo. O número máximo de pares BGP dinâmicos é 512.

Para criar um par BGP:

1. Crie um par BGP de uma das seguintes formas:

   - Para criar um par BGP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BGP → Vizinhos**.

   - Para criar um par BGP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **BGP → Vizinhos** e marque a caixa de seleção **Substituir**.

   Uma tabela de pares BGP é exibida.

2. Clique em **+ Vizinho BGP**.

3. Na janela aberta, no campo **Nome**, insira o nome do par BGP. O comprimento máximo do nome é de 50 caracteres.

4. Para desativar um par BGP e impedir o estabelecimento de uma sessão TCP com ele, marque a caixa de seleção **Desativar par BGP**. Esta caixa de seleção está desmarcada por padrão.

5. No campo **IP do vizinho**, insira o endereço IPv4 do par BGP.

6. No campo **AS remoto**, insira o número do sistema autônomo do par BGP. Intervalo de valores: 1 a 4.294.967.295.

7. Se necessário, insira uma breve descrição do par BGP no campo **Descrição**.

8. Se desejar que o dispositivo CPE use uma senha ao estabelecer uma sessão TCP com o par BGP, insira a senha no campo **Senha**. Para que uma sessão TCP seja estabelecida entre dois pares BGP, eles devem usar a mesma senha. Para ver a senha inserida, clique no ícone de exibição .

9. Se necessário, no campo **Fonte de atualização**, insira o endereço IPv4 da interface de loopback que o dispositivo CPE envia ao par BGP ao estabelecer uma sessão TCP.

10. Se a sessão TCP não for estabelecida diretamente entre o dispositivo CPE e o par BGP, no campo **Saltos do eBGP**, insira o número de saltos entre o dispositivo CPE e o par BGP. Intervalo de valores: 1 a 255.

11. Para configurar temporizadores do BGP:

    a. Marque a caixa de seleção **Temporizadores do BGP personalizados**. Esta caixa de seleção está desmarcada por padrão.

    b. No campo **Keepalive (s)**, insira o intervalo de tempo em segundos que o dispositivo CPE usa para enviar pacotes de controle ao par BGP. Intervalo de valores: 0 a 65.535.

    c. No campo **Tempo de espera (s)**, insira o intervalo de tempo em segundos que o dispositivo CPE usa ao receber pacotes de controle do par BGP. Se nenhum pacote de controle for recebido do par BGP dentro do tempo especificado, o dispositivo CPE considera esse par BGP indisponível. Intervalo de valores: 0 a 65.535.

12. Para usar o protocolo BFD para detectar a perda de conexão, marque a caixa de seleção **BFD**. Esta caixa de seleção está desmarcada por padrão. Quando a caixa de seleção é marcada, as alterações feitas no mapa de roteamento são imediatamente aplicadas a um par BGP caso o par BGP use esse mapa de roteamento. Para selecionar um mapa de roteamento para o par BGP, veja a etapa 14 destas instruções.

13. Para especificar configurações avançadas para o par BGP:

    a. Selecione a guia **Configurações avançadas**.

    As configurações avançadas do par BGP são exibidas.

    b. Se necessário, marque as seguintes caixas de seleção:

    - Marque a caixa de seleção **Recuperação suave de entrada** para armazenar rotas anunciadas pelo par BGP localmente no dispositivo CPE. O uso desse recurso reduz a quantidade de memória disponível no dispositivo CPE. Quando a caixa de seleção é marcada, as alterações feitas no mapa de roteamento são imediatamente aplicadas a um par BGP caso o par BGP use esse mapa de roteamento. Para selecionar um mapa de roteamento para o par BGP, veja a etapa 14 destas instruções.
    - Marque a caixa de seleção **Atributo inalterado AS path** para impedir a modificação do atributo 'AS path' das rotas que o dispositivo CPE anuncia para o par BGP.
    - Marque a caixa de seleção **Permitir AS em** para permitir que os pares BGP anunciem rotas para o dispositivo CPE com o atributo 'AS path', cujo valor é o número do sistema autônomo do dispositivo CPE.
    - Marque a caixa de seleção **Atributo inalterado next-hop** para impedir a modificação do atributo 'next hop' das rotas que o dispositivo CPE anuncia para o par BGP.
    - Marque a caixa de seleção **Next-hop self** para usar o endereço IPv4 do dispositivo CPE como o valor do atributo 'next hop' ao anunciar rotas para o par BGP.
    - Marque a caixa de seleção **Atributo inalterado MED** para impedir a modificação do atributo 'MED' das rotas que o dispositivo CPE anuncia para o par BGP.
    - Marque a caixa de seleção **Cliente refletor de rotas** para atribuir a função de *Refletor de rotas* ao dispositivo CPE e a função de *Cliente do refletor de rotas* ao par BGP. Essa caixa de seleção só pode ser marcada para um par BGP que esteja no mesmo sistema autônomo que o dispositivo CPE.

    Essas caixas de seleção são desmarcadas por padrão.

    c. No campo **AS local**, insira o número do sistema autônomo local que o dispositivo CPE envia ao par BGP. Intervalo de valores: 1 a 4.294.967.295.

    d. No campo **Peso**, insira o peso das rotas anunciadas pelo par BGP. Quanto maior o peso de uma rota, maior sua prioridade. Intervalo de valores: 0 a 65.535.

    e. No campo **Prefixo máximo**, insira o número máximo de rotas que o par BGP pode anunciar para um dispositivo CPE. Intervalo de valores: 1 a 4.294.967.295.

    f. Para que um dispositivo CPE anuncie rotas com o atributo 'community' para seu par BGP, marque a caixa de seleção **Enviar comunidade** e selecione o tipo do atributo na lista suspensa:

    - **Todos** abrange todos os tipos disponíveis do atributo 'community'.
    - **Comunidade estendida e padrão**.
    - **Comunidade estendida**.

- **Grande comunidade**.
- **Comunidade padrão**.

Esta caixa de seleção está desmarcada por padrão.

a. Para que o dispositivo CPE anuncie a rota padrão 0.0.0.0/0 para o par BGP, marque a caixa de seleção **Originar padrão**. Esta caixa de seleção está desmarcada por padrão. Marque a caixa de seleção **Definir mapa de roteamento** e, na lista suspensa exibida, selecione o mapa de roteamento criado para a rota padrão 0.0.0.0/0.

14. Para configurar a filtragem de rotas para o par BGP:

a. Selecione a guia **Filtragem**.

As configurações de filtragem de rotas são exibidas.

b. Em **Mapa de roteamento**, selecione os mapas de roteamento criados:

1. Na lista suspensa **De entrada**, selecione um mapa de roteamento para as rotas que o par BGP anuncia para o dispositivo CPE.
2. Na lista suspensa **De saída**, selecione um mapa de roteamento para as rotas que o dispositivo CPE anuncia para o par BGP.

c. Em **Lista de prefixos**, selecione as listas de prefixos criadas:

1. Na lista suspensa **De entrada**, selecione uma lista de prefixos para as rotas que o par BGP anuncia para o dispositivo CPE.
2. Na lista suspensa **De saída**, selecione uma lista de prefixos para as rotas que o dispositivo CPE anuncia para o par BGP.

d. Em **Lista de controle de acesso**, selecione as listas de controle de acesso criadas:

1. Na lista suspensa **De entrada**, selecione uma lista de controle de acesso para as rotas que o par BGP anuncia para o dispositivo CPE.
2. Na lista suspensa **De saída**, selecione uma lista de controle de acesso para as rotas que o dispositivo CPE anuncia para o par BGP.

15. Clique em **Criar**.

O par BGP é criado e exibido na tabela.

16. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar um par BGP

É possível editar um par BGP em um modelo de CPE ou dispositivo CPE. Um par BGP editado no modelo de CPE é editado automaticamente em todos os dispositivos CPE que usam o modelo. Não é possível editar um par BGP herdado de um modelo de CPE em um dispositivo CPE.

Para editar um par BGP:

1. Edite um par BGP de uma das seguintes formas:

   - Para editar um par BGP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BGP → Vizinhos**.

   - Para editar um par BGP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **BGP → Vizinhos** e marque a caixa de seleção **Substituir**.

   Uma tabela de pares BGP é exibida.

2. Clique em **Editar** ao lado do par BGP que deseja editar.

3. Na janela aberta, se necessário, edite as configurações do par BGP. Para obter uma descrição das configurações, consulte as instruções para criar um par BGP.

4. Clique em **Salvar**.

   O par BGP é modificado e atualizado na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir um par BGP

É possível excluir um par BGP em um modelo de CPE ou dispositivo CPE. Um par BGP excluído do modelo de CPE é excluído automaticamente de todos os dispositivos CPE que usam o modelo. Não é possível excluir um par BGP herdado de um modelo de CPE em um dispositivo CPE.

Os pares BGP excluídos não podem ser restaurados.

Para excluir um par BGP:

1. Exclua um par BGP de uma das seguintes formas:

   - Para excluir um par BGP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BGP → Vizinhos**.

   - Para excluir um par BGP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **BGP → Vizinhos** e marque a caixa de seleção **Substituir**.

   Uma tabela de pares BGP é exibida.

2. Clique em **Excluir** ao lado do par BGP que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   O par BGP é excluído e não é mais exibido na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar grupos de pares BGP

Para visualizar ou editar a tabela de grupos de pares BGP de uma instância BGP em um modelo de CPE ou em um dispositivo CPE:

1. Vá para a seção **BGP**. Para isso:

   - Para visualizar ou editar a tabela de grupos de pares BGP em um modelo de CPE , vá para a seção **SD-WAN→ Modelos de CPE** do menu, clique no modelo de CPE e, na barra lateral da área de configurações, selecione **BGP**.

   - Para visualizar ou editar a tabela de grupos de pares BGP em um dispositivo CPE, vá para a seção **SD-WAN→ CPE** do menu, clique no dispositivo CPE e, na barra lateral da área de configurações, clique em **BGP**.

2. Abra uma instância BGP existente clicando em **Editar** na linha correspondente da tabela ou crie uma nova instância BGP.

3. Na área de configurações da instância BGP, selecione a guia **Grupos de pares**.

As informações sobre grupos de pares BGP são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do grupo de pares BGP.
- **Intervalo do BGP** é o prefixo IPv4 do grupo de pares BGP.
- **Descrição** é uma breve descrição do grupo de pares BGP.
- **Herdado** indica se o grupo de pares BGP é herdado do modelo de CPE:

  - **Sim**.
  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.

- **AS remoto** é o número do sistema autônomo do grupo de pares BGP.
- **Desligar** indica se o grupo de pares BGP está desativado e nenhuma sessão TCP foi estabelecida com ele.

  - **Sim**.
  - **Não**.

- **Peso** é o peso das rotas anunciadas pelo grupo de pares BGP.
- **Gerenciamento** contém as ações que podem ser executadas com o grupo de pares BGP.

Criar um grupo de pares BGP

É possível criar um grupo de pares BGP em um modelo de CPE ou dispositivo CPE. Grupos de pares BGP criados no modelo de CPE são criados automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar um grupo de pares BGP:

1. Crie um grupo de pares BGP de uma das seguintes formas:

   - Para criar um grupo de pares BGP em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BGP** → **Grupos de pares**.

   - Para criar um grupo de pares BGP em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **BGP** → **Grupos de pares** e marque a caixa de seleção **Substituir**.

   Uma tabela de grupos de pares BGP é exibida.

2. Clique em **+ Grupo de pares**.

3. Na janela aberta, no campo **Nome**, insira o nome do grupo de pares BGP. O comprimento máximo do nome é de 50 caracteres.

4. Para desativar um grupo de pares BGP e impedir o estabelecimento de uma sessão TCP com ele, marque a caixa de seleção **Desativar grupo de pares BGP**. Esta caixa de seleção está desmarcada por padrão.

5. No campo **Intervalo do BGP**, insira o endereço IPv4 do grupo de pares BGP.

6. No campo **AS remoto**, insira o número do sistema autônomo do grupo de pares BGP. Intervalo de valores: 1 a 4.294.967.295.

7. Se necessário, insira uma breve descrição do grupo de pares BGP no campo **Descrição**.

8. Se desejar que o dispositivo CPE use uma senha ao estabelecer uma sessão TCP com o grupo de pares BGP, insira a senha no campo **Senha**. Para que uma sessão TCP seja estabelecida entre dois pares BGP, eles devem usar a mesma senha. Para ver a senha inserida, clique no ícone de exibição 👁.

9. No campo **Fonte de atualização**, insira o endereço IPv4 da interface de loopback que o dispositivo CPE envia ao grupo de pares BGP ao estabelecer uma sessão TCP.

10. Se a sessão TCP não for estabelecida diretamente entre o dispositivo CPE e o grupo de pares BGP, no campo **Saltos do eBGP**, insira o número de saltos entre o dispositivo CPE e o grupo de pares BGP. Intervalo de valores: 1 a 255.

11. Para configurar temporizadores do BGP:

    a. Marque a caixa de seleção **Temporizadores do BGP personalizados**. Esta caixa de seleção está desmarcada por padrão.

    b. No campo **Keepalive (s)**, insira o intervalo de tempo em segundos que o dispositivo CPE usa para enviar pacotes de controle ao grupo de pares BGP. Intervalo de valores: 0 a 65.535.

    c. No campo **Tempo de espera (s)**, insira o intervalo de tempo em segundos que o dispositivo CPE usa ao receber pacotes de controle do grupo de pares BGP. Se nenhum pacote de controle for recebido do par BGP dentro do tempo especificado, o dispositivo CPE considera esse par BGP indisponível. Intervalo de valores: 0 a 65.535.

12. Para usar o protocolo BFD para detectar a perda de conexão, marque a caixa de seleção **BFD**. Esta caixa de seleção está desmarcada por padrão. Quando a caixa de seleção é marcada, as alterações feitas no mapa de roteamento são imediatamente aplicadas a um grupo de pares BGP caso o grupo de pares BGP use esse mapa de roteamento. Para selecionar um mapa de roteamento para o grupo de pares BGP, veja a etapa 14 destas instruções.

13. Para especificar configurações avançadas para o grupo de pares BGP:

    a. Selecione a guia **Configurações avançadas**.

    As configurações avançadas do grupo de pares BGP são exibidas.

    b. Se necessário, marque as seguintes caixas de seleção:

    - Marque a caixa de seleção **Recuperação suave de entrada** para armazenar rotas anunciadas pelo grupo de pares BGP localmente no dispositivo CPE. O uso desse recurso reduz a quantidade de memória disponível no dispositivo CPE. Quando a caixa de seleção é marcada, as alterações feitas no mapa de roteamento são imediatamente aplicadas a um grupo de pares BGP caso o grupo de pares BGP use esse mapa de roteamento. Para selecionar um mapa de roteamento para o grupo de pares BGP, veja a etapa 14 destas instruções.
    - Marque a caixa de seleção **Atributo inalterado AS path** para impedir a modificação do atributo 'AS path' das rotas que o dispositivo CPE anuncia para o grupo de pares BGP.
    - Marque a caixa de seleção **Permitir AS em** para permitir que o grupo de pares BGP anuncie rotas para o dispositivo CPE com o atributo 'AS path', cujo valor é o número do sistema autônomo do dispositivo CPE.
    - Marque a caixa de seleção **Atributo inalterado next-hop** para impedir a modificação do atributo 'next hop' das rotas que o dispositivo CPE anuncia para o grupo de pares BGP.
    - Marque a caixa de seleção **Next-hop self** para usar o endereço IPv4 do dispositivo CPE como o valor do atributo 'next hop' ao anunciar rotas para o grupo de pares BGP.
    - Marque a caixa de seleção **Atributo inalterado MED** para impedir a modificação do atributo 'MED' das rotas que o dispositivo CPE anuncia para o grupo de pares BGP.
    - Marque a caixa de seleção **Cliente refletor de rotas** para atribuir a função de *Refletor de rotas* ao dispositivo CPE e a função de *Cliente do refletor de rotas* ao grupo de pares BGP. Essa caixa de seleção só pode ser marcada para um grupo de pares BGP que esteja no mesmo sistema autônomo que o dispositivo CPE.

    Essas caixas de seleção são desmarcadas por padrão.

c. No campo **AS local**, insira o número do sistema autônomo local que o dispositivo CPE envia ao grupo de pares BGP. Intervalo de valores: 1 a 4.294.967.295.

d. No campo **Peso**, insira o peso das rotas anunciadas pelo grupo de pares BGP. Quanto maior o peso de uma rota, maior sua prioridade. Intervalo de valores: 0 a 65.535.

e. No campo **Prefixo máximo**, insira o número máximo de rotas que o grupo de pares BGP pode anunciar para um dispositivo CPE. Intervalo de valores: 1 a 4.294.967.295.

f. Para que um dispositivo CPE anuncie rotas com o atributo 'community' para o grupo de pares BGP, marque a caixa de seleção **Enviar comunidade** e selecione o tipo do atributo a ser enviado na lista suspensa:

- **Todos** abrange todos os tipos disponíveis do atributo 'community'.
- **Comunidade estendida e padrão**.
- **Comunidade estendida**.
- **Grande comunidade**.
- **Comunidade padrão**.

Esta caixa de seleção está desmarcada por padrão.

a. Para que o dispositivo CPE anuncie a rota padrão 0.0.0.0/0 para o grupo de pares BGP, marque a caixa de seleção **Originar padrão**. Esta caixa de seleção está desmarcada por padrão. Marque a caixa de seleção **Definir mapa de roteamento** e, na lista suspensa exibida, selecione o mapa de roteamento criado para a rota padrão 0.0.0.0/0.

14. Para configurar a filtragem de rotas para o grupo de pares BGP:

a. Selecione a guia **Filtragem**.

As configurações de filtragem de rotas são exibidas.

b. Em **Mapa de roteamento**, selecione os mapas de roteamento criados:

1. Na lista suspensa **De entrada**, selecione um mapa de roteamento para as rotas que o grupo de pares BGP anuncia para o dispositivo CPE.
2. Na lista suspensa **De saída**, selecione um mapa de roteamento para as rotas que o dispositivo CPE anuncia para o grupo de pares BGP.

c. Em **Lista de prefixos**, selecione as listas de prefixos criadas:

1. Na lista suspensa **De entrada**, selecione uma lista de prefixos que o grupo de pares BGP anuncia para o dispositivo CPE.
2. Na lista suspensa **De saída**, selecione uma lista de prefixos para as rotas que o dispositivo CPE anuncia para o grupo de pares BGP.

d. Em **Lista de controle de acesso**, selecione as listas de controle de acesso criadas:

1. Na lista suspensa **De entrada**, selecione uma lista de controle de acesso para as rotas que o grupo de pares BGP anuncia para o dispositivo CPE.

2. Na lista suspensa **De saída**, selecione uma lista de controle de acesso para as rotas que o dispositivo CPE anuncia para o grupo de pares BGP.

15. Clique em **Criar**.

    O grupo de pares BGP é criado e exibido na tabela.

16. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar um grupo de pares BGP

É possível editar um grupo de pares BGP em um modelo de CPE ou dispositivo CPE. Um grupo de pares BGP editado no modelo de CPE é editado automaticamente em todos os dispositivos CPE que usam o modelo. Não é possível editar um grupo de pares BGP herdado de um modelo de CPE em um dispositivo CPE.

Para editar um grupo de pares BGP:

1. Edite um grupo de pares BGP de uma das seguintes formas:

   - Para editar um grupo de pares BGP em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BGP** → **Grupos de pares**.

   - Para editar um grupo de pares BGP em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **BGP** → **Grupos de pares** e marque a caixa de seleção **Substituir**.

   Uma tabela de grupos de pares BGP é exibida.

2. Clique em **Editar** ao lado do grupo de pares BGP que deseja editar.

3. Na janela aberta, se necessário, edite as configurações do grupo de pares BGP. Para obter uma descrição das configurações, consulte as instruções para criar um grupo de pares BGP.

4. Clique em **Salvar**.

   O grupo de pares BGP é modificado e atualizado na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir um grupo de pares BGP

É possível excluir um grupo de pares BGP em um modelo de CPE ou dispositivo CPE. Um grupo de pares BGP excluído do modelo de CPE é excluído automaticamente de todos os dispositivos CPE que usam o modelo. Não é possível excluir um grupo de pares BGP herdado de um modelo de CPE em um dispositivo CPE.

Os grupos de pares BGP excluídos não podem ser restaurados.

Para excluir um grupo de pares BGP:

1. Exclua um grupo de pares BGP de uma das seguintes formas:

   - Para excluir um grupo de pares BGP em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BGP** → **Grupos de pares**.
   - Para excluir um grupo de pares BGP em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **BGP** → **Grupos de pares** e marque a caixa de seleção **Substituir**.

   Uma tabela de grupos de pares BGP é exibida.

2. Clique em **Excluir** ao lado do grupo de pares BGP que deseja excluir.
3. Na janela de confirmação, clique em **Excluir**.

   O grupo de pares BGP é excluído e não é mais exibido na tabela.
4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Configurar vazamento de rota inter-VRF

Para visualizar ou editar o Vazamento de Rota Inter-VRF para uma instância BGP em um modelo de CPE ou em um dispositivo CPE:

1. Vá para a seção **BGP**. Para isso:

   - Para visualizar ou editar as configurações de Vazamento de Rota Inter-VRF em um modelo de CPE , vá para a seção **SD-WAN**→ **Modelos de CPE** do menu, clique no modelo de CPE e, na barra lateral da área de configurações, selecione **BGP**.
   - Para visualizar ou editar as configurações de Vazamento de Rota Inter-VRF em um dispositivo CPE, vá para a seção **SD-WAN**→ **CPE** do menu, clique no dispositivo CPE e, na barra lateral da área de configurações, clique em **BGP**.

2. Abra uma instância BGP existente clicando em **Editar** na linha correspondente da tabela ou crie uma nova instância BGP.
3. Na área de configurações da instância BGP, selecione a guia **Vazamento de rotas**.

4. Se necessário, gerencie as seguintes configurações de Vazamento de Rota Inter-VRF:

   - No campo **Diferenciador de rotas**, especifique o atributo Diferenciador de rotas (RD) para o vazamento de rota (um ID exclusivo para distinguir rotas). Ele pode ser especificado em um de dois formatos:

     - Número do sistema autônomo (de 0 a 4294967295): ID (de 0 a 65535). Exemplo: `100:65000`.
     - Endereço IPv4: ID (de 0 a 65535) Exemplo: `1.2.3.4:15`.

     O atributo Diferenciador de rotas pode ser gerado automaticamente ao marcar a caixa de seleção **Geração automática** (marcada por padrão).

   - Em **Exportação de destino de rotas**, clique em **Adicionar** para adicionar um ou mais valores de Destino de rota (RT) para exportar rotas do VRF desta instância BGP para outros VRFs.
   - Em **Importação de destino de rotas**, clique **Adicionar** para adicionar um ou mais valores de Destino de rota (RT) para importar rotas para o VRF desta instância BGP de outros VRFs.

     Os valores de entrada de Destino de rota individual para as configurações **Exportação de destino de rotas** e **Importação de destino de rotas** são especificados em um de dois formatos:

     - Número do sistema autônomo (de 0 a 4294967295): ID (de 0 a 65535). Exemplo: `100:3000`.
     - Endereço IPv4: ID (de 0 a 65535) Exemplo: `6.6.6.6:77`.

   - Ative o botão **Exportar rotas** caso precise exportar rotas do VRF desta instância BGP.
   - Ative o botão **Importar rotas**caso precise importar rotas para o VRF desta instância BGP.
   - Nas listas **Exportar mapa de roteamento** e **Importar mapa de roteamento**, selecione os mapas de roteamento criados para rotas exportadas e importadas.

5. Clique em **Salvar** para salvar as alterações, ou em **Cancelar** para descartar as alterações.

Troca de rotas por OSPF

O Kaspersky SD-WAN é compatível com o protocolo de roteamento dinâmico OSPF (Open Shortest Path First) para a troca de informações de roteamento entre dispositivos CPE e dispositivos de rede externos. Ao configurar o protocolo OSPF, é possível usar áreas OSPF e interfaces OSPF.

Configurações básicas do OSPF

É possível especificar configurações básicas do OSPF em um modelo de CPE ou dispositivo CPE. As configurações básicas do OSPF especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para modificar as configurações básicas do OSPF:

1. Especifique as configurações básicas do OSPF de uma das seguintes formas:

   - Para editar as configurações básicas do OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF**.
   - Para editar as configurações básicas do OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **OSPF** e marque a caixa de seleção **Substituir**.

   Por padrão, é selecionada a guia **Configurações gerais**, que exibe as configurações do OSPF.

2. Na lista suspensa **OSPF**, selecione **Ativado**. O valor padrão é **Desativado**.
3. No campo **ID do roteador**, insira o endereço IPv4 que deseja atribuir ao ID do roteador do dispositivo CPE.
4. No campo **Máximo de caminhos**, insira o número máximo de entradas na tabela de roteamento e encaminhamento do dispositivo CPE. Intervalo de valores: 1 a 16.
5. Para usar o dispositivo CPE como um roteador de borda de área (ABR), na lista suspensa **Tipo de ABR**, selecione uma das seguintes implementações:

   - **IBM** (implementação padrão)
   - **CISCO**
   - **SHORTCUT**
   - **STANDARD**

6. No campo **Largura de banda de referência automática de custo**, insira a largura de banda de referência para calcular o custo dos links no dispositivo CPE. Intervalo de valores: 1 a 4.294.967.
7. Para mudar todas as interfaces OSPF do dispositivo CPE para o modo passivo, marque a caixa de seleção **Interface passiva padrão**. No modo passivo, as interfaces OSPF não trocam pacotes de tráfego. Esta caixa de seleção está desmarcada por padrão.
8. Para manter um log do OSPF, marque a caixa de seleção **Registrar alterações de adjacências**. É possível marcar a caixa de seleção **Detalhe** para manter um log do OSPF mais detalhado. Essas caixas de seleção são desmarcadas por padrão.
9. Para configurar a redistribuição de rotas no OSPF, em **Redistribuição de rotas**, faça o seguinte:

   a. Marque as caixas de seleção ao lado dos tipos de rota:

      - **BGP** para redistribuir rotas BGP.
      - **Conectado** para redistribuir rotas diretamente conectadas às interfaces de rede do dispositivo CPE.
      - **Kernel** para redistribuir as rotas do Kernel geradas pelo sistema operacional do dispositivo CPE.
      - **Estática** para redistribuir rotas estáticas.

      Essas caixas de seleção são desmarcadas por padrão.

   b. Na lista suspensa **Mapa de roteamento**, selecione um mapa de roteamento criado para rotas redistribuídas.

c. No campo **Métrica**, insira uma métrica de rotas redistribuídas. Intervalo de valores: 0 a 16.777.214.

d. Na lista suspensa **Tipo de métrica**, selecione o tipo da métrica:

- **Tipo 1** (ou "métrica interna")
- **Tipo 2** (ou "métrica externa")

e. Marque a caixa de seleção **Filtragem** e, na lista suspensa **Lista de controle de acesso**, selecione uma lista de controle de acesso criada para rotas realocadas. Esta caixa de seleção está desmarcada por padrão.

10. No campo **Métrica padrão**, insira a métrica padrão de rotas OSPF. Intervalo de valores: 0 a 16.777.214.

11. Para configurar que o dispositivo CPE anuncie a rota padrão 0.0.0.0/0 para vizinhos OSPF:

a. Marque a caixa de seleção **Originar padrão**. Esta caixa de seleção está desmarcada por padrão.

b. Marque a caixa de seleção **Sempre** para sempre anunciar a rota 0.0.0.0/0 padrão, mesmo se ela não estiver presente na tabela de rotas do dispositivo CPE. Esta caixa de seleção está desmarcada por padrão.

c. Na lista suspensa **Tipo de métrica**, selecione o tipo de métrica para a rota padrão 0.0.0.0/0:

- **Tipo 1**
- **Tipo 2**

d. No campo **Métrica**, insira uma métrica para a rota padrão 0.0.0.0/0. Intervalo de valores: 0 a 16.777.214.

e. Na lista suspensa **Mapa de roteamento**, selecione um mapa de roteamento criado para a rota padrão 0.0.0.0/0.

12. No campo **Distância**, insira a distância administrativa para todas as rotas OSPF. Quanto menor a distância administrativa especificada para um protocolo, maior a prioridade de sua rota. Por exemplo, caso deseje que as rotas OSPF sempre tenham preferência sobre as rotas BGP, especifique a distância administrativa de 1 para OSPF e 2 para BGP. Intervalo de valores: 1 a 255.

13. Para configurar distâncias administrativas para rotas OSPF individuais:

a. Marque a caixa de seleção **Distância OSPF**. Esta caixa de seleção está desmarcada por padrão.

b. No campo **Externo**, insira a distância administrativa para rotas de domínios OSPF externos ou protocolos de roteamento. Intervalo de valores: 1 a 255.

c. No campo **Interárea**, insira a distância administrativa para rotas de diferentes áreas OSPF do mesmo domínio OSPF. Intervalo de valores: 1 a 255.

d. No campo **Intra-área**, insira a distância administrativa para rotas da mesma área OSPF. Intervalo de valores: 1 a 255.

14. Para ativar a reinicialização normal no dispositivo CPE:

a. Marque a caixa de seleção **Reinicialização normal**. Esta caixa de seleção está desmarcada por padrão.

b. No campo **Período de carência (s)**, insira o tempo, em segundos, durante o qual o dispositivo CPE anuncia sua intenção de reiniciar aos vizinhos OSPF. Intervalo de valores: 1 a 1800.

15. Para configurar temporizadores para os cálculos do algoritmo Shortest Path First (SPF):

    a. Marque a caixa de seleção **Temporizador de limitação de SPF**. Esta caixa de seleção está desmarcada por padrão.

    b. No campo **Atraso (ms)**, insira a duração, em milissegundos, do atraso antes de iniciar os cálculos do algoritmo SPF. Intervalo de valores: 0 a 600.000.

    c. No campo **Tempo de retenção inicial (ms)**, insira o tempo mínimo de retenção, em milissegundos, entre dois cálculos do algoritmo SPF. Intervalo de valores: 0 a 600.000.

    d. No campo **Tempo máximo de retenção (ms)**, insira o tempo máximo de retenção, em milissegundos, entre dois cálculos do algoritmo SPF. Intervalo de valores: 0 a 600.000.

16. Para configurar o Anúncio de estado de link (LSA) a vizinhos OSPF para o dispositivo CPE:

    a. Marque a caixa de seleção **Administrativo** para que o dispositivo CPE use a métrica máxima em anúncios de estado de link para vizinhos OSPF.

    b. Para especificar durante quanto tempo o dispositivo CPE deve usar a métrica máxima no anúncio de estado de link para vizinhos OSPF quando o protocolo OSPF é iniciado ou reiniciado:

        1. Marque a caixa de seleção **Na inicialização**. Esta caixa de seleção está desmarcada por padrão.

        2. No campo **Temporizador (s)**, insira o tempo em segundos. Intervalo de valores: 5 a 86.400.

    c. Para especificar durante quanto tempo o dispositivo CPE deve usar a métrica máxima no anúncio de estado de link para vizinhos OSPF quando o protocolo OSPF é desativado:

        1. Marque a caixa de seleção **No desligamento**. Esta caixa de seleção está desmarcada por padrão.

        2. No campo **Temporizador (s)**, insira o tempo em segundos. Intervalo de valores: 5 a 100.

17. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar áreas OSPF

É possível visualizar a tabela de áreas OSPF em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de áreas OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF → Áreas OSPF**.

- Para visualizar a tabela de áreas OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **OSPF → Áreas OSPF**.

As informações sobre as áreas OSPF são exibidas nas seguintes colunas da tabela:

- **Área OSPF** é o ID da área OSPF na forma de um endereço IPv4 ou um número inteiro.
- **Tipo de área** é o tipo de área OSPF stub:
  - **Stub**
  - **Stub NO-SUMMARY**
  - **NSSA**
  - **NSSA NO-SUMMARY**

  Esse valor é exibido apenas para áreas stub.
- **Intervalos OSPF** especifica intervalos OSPF.
- **Gerenciamento** contém as ações que podem ser executadas com a área OSPF.

Criar uma área OSPF

É possível criar uma área OSPF em um modelo de CPE ou dispositivo CPE. OSPFs criados no modelo de CPE são criados automaticamente em todos os dispositivos CPE aos quais esse modelo de CPE está aplicado.

Para criar uma área OSPF:

1. Crie uma área OSPF de uma das seguintes formas:
   - Para criar uma área OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF → Áreas OSPF**.
   - Para criar uma área OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **OSPF → Áreas OSPF** e marque a caixa de seleção **Substituir**.

   Uma tabela de áreas OSPF é exibida.
2. Clique em **+ Área OSPF**.
3. Na janela aberta, no campo **Área OSPF**, insira o ID da área OSPF como um endereço IPv4 ou um número inteiro.
4. Para tornar a área OSPF uma área stub:
   a. Marque a caixa de seleção **Stub**. Esta caixa de seleção está desmarcada por padrão.
   b. Na lista suspensa **Tipo de área**, selecione o tipo da área OSPF stub:
      - **Stub**
      - **Stub NO-SUMMARY**
      - **NSSA**
      - **NSSA NO-SUMMARY**

c. Caso tenha selecionado **NSSA** ou **NSSA NO-SUMMARY** na lista suspensa **Tipo de área** e precisar impedir a divulgação da rota padrão 0.0.0.0/0 para a área NSSA, marque a caixa de seleção **Suprimir FA em NSSA**. Esta caixa de seleção está desmarcada por padrão.

d. No campo **Custo padrão**, insira uma métrica para a rota padrão ou para rotas de resumo. Intervalo de valores: 0 a 16.777.215.

5. Para usar o método de atalho para cálculos de SPF, marque a caixa de seleção **Atalho**. Esta caixa de seleção está desmarcada por padrão.

6. Na lista suspensa **Autenticação**, selecione o método de autenticação OSPF:

   - **Função hash** para usar o algoritmo MD5.
   - **Senha** para usar uma senha não criptografada. Esse método de autenticação é menos seguro que o algoritmo MD5, no entanto, pode fornecer autenticação quando usado em um ambiente de rede confiável.

7. Para especificar intervalos OSPF:

   a. Em **Intervalos OSPF**, clique em **+ Intervalo**.

   b. No campo **Intervalo**, insira o prefixo IPv4 das rotas.

   c. Na lista suspensa **Ação**, selecione a ação a ser executada com as rotas:

      - **Anunciar** para anunciar as rotas através do protocolo OSPF. Essa é a configuração padrão.
      - **Não anunciar** para não anunciar as rotas através do protocolo OSPF.
      - **Substituir** para substituir o prefixo IPv4 das rotas pelo prefixo IPv4 especificado e, em seguida, anunciá-los através do protocolo OSPF. Ao selecionar esse valor, insira o prefixo IPv4 no campo **Substituir**.

   d. Caso tenha selecionado **Anunciar** ou **Substituir** na lista suspensa **Ação**, no campo **Custo**, insira uma métrica para as rotas. Intervalo de valores: 0 a 16.777.215.

   O intervalo OSPF é especificado e exibido em **Intervalos OSPF**. É possível especificar vários intervalos OSPF ou excluir intervalos OSPF. Para excluir um intervalo OSPF, clique no ícone de exclusão ✕ ao lado dele.

8. Para conectar uma área OSPF a outra área OSPF por meio de uma área OSPF de trânsito, especifique o link virtual:

   a. Em **Links virtuais**, clique em **+ Link virtual**.

   b. No campo **Endereço**, insira o endereço IPv4 da interface de rede do roteador na área de trânsito.

   O link virtual é especificado e exibido em **Intervalos OSPF**. É possível especificar vários links virtuais ou excluir links virtuais. Para excluir um link virtual, clique no ícone de exclusão ✕ ao lado dele.

9. Para configurar a filtragem de rotas para a área OSPF, em **Filtragem**, faça o seguinte:

    a. Selecione as listas de controle de acesso criadas:

        1. Na lista suspensa **Lista de exportação**, selecione uma lista de controle de acesso para rotas anunciadas da área OSPF para outras áreas OSPF.

        2. Na lista suspensa **Lista de importação**, selecione uma lista de controle de acesso para rotas anunciadas de outra área OSPF para a área OSPF especificada.

    b. Selecione as listas de acesso criadas:

        1. Na lista suspensa **Lista de filtros de saída**, selecione uma lista de prefixos para rotas anunciadas da área OSPF para outras áreas OSPF.

        2. Na lista suspensa **Lista de filtros de entrada**, selecione uma lista de prefixos para rotas anunciadas de outra área OSPF para a área OSPF especificada.

10. Clique em **Salvar**.

    A área OSPF é criada e exibida na tabela.

11. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma área OSPF

É possível editar uma área OSPF em um modelo de CPE ou dispositivo. Uma área OSPF editada no modelo de CPE é editada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma área OSPF:

1. Edite uma área OSPF de uma das seguintes formas:

    - Para editar uma área OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF → Áreas OSPF**.
    - Para editar uma área OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **OSPF → Áreas OSPF** e marque a caixa de seleção **Substituir**.

    Uma tabela de áreas OSPF é exibida.

2. Clique em **Editar** ao lado da área OSPF que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da área OSPF. Para obter uma descrição das configurações, consulte as instruções para criar uma área OSPF.

4. Clique em **Salvar**.

    A área OSPF é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma área OSPF

É possível excluir uma área OSPF em um modelo de CPE ou dispositivo CPE. Uma área OSPF excluída no modelo de CPE é excluída automaticamente em todos os dispositivos CPE que usam o modelo.

As áreas OSPF excluídas não podem ser restauradas.

Para excluir uma área OSPF:

1. Exclua uma área OSPF de uma das seguintes formas:

   - Para excluir uma área OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF → Áreas OSPF**.
   - Para excluir uma área OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **OSPF → Áreas OSPF** e marque a caixa de seleção **Substituir**.

   Uma tabela de áreas OSPF é exibida.

2. Clique em **Excluir** ao lado da área OSPF que deseja excluir.
3. Na janela de confirmação, clique em **Excluir**.

   A área OSPF é excluída e não é mais exibida na tabela.
4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar interfaces OSPF

É possível visualizar a tabela de interfaces OSPF em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de interfaces OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF → Interfaces OSPF**.
- Para visualizar a tabela de interfaces OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **OSPF → Interfaces OSPF**.

As informações sobre as interfaces OSPF são exibidas nas seguintes colunas da tabela:

- **Interface** é a interface de rede usada como interface OSPF.
- **Área OSPF** é o ID da área OSPF à qual a interface pertence.
- **Autenticação** é o método de autenticação.
- **Tipo de rede** é o tipo de rede à qual a interface OSPF está conectada.
- **Gerenciamento** contém as ações que podem ser executadas com a interface OSPF.

Criar uma interface OSPF

É possível criar uma interface OSPF em um modelo de CPE ou dispositivo CPE. Interfaces OSPF criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma interface OSPF:

1. Crie uma interface OSPF de uma das seguintes formas:

   - Para criar uma interface OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF → Interfaces OSPF**.
   - Para criar uma interface OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **OSPF → Interfaces OSPF** e marque a caixa de seleção **Substituir**.

   Uma tabela de interfaces OSPF é exibida.

2. Clique em **+ Interface OSPF**.
3. Na janela aberta, na lista suspensa **Interface**, selecione a interface de rede criada que deseja usar como interface OSPF.
4. No campo **Área OSPF**, insira o ID da área OSPF à qual a interface OSPF pertence, na forma de um endereço IPv4 ou um número inteiro.
5. Para especificar a autenticação OSPF:

   a. Na lista suspensa **Autenticação**, selecione um método de autenticação:

      - **Função hash** para usar o algoritmo MD5.
      - **Senha** para usar uma senha não criptografada. Esse método de autenticação é menos seguro que o algoritmo MD5, no entanto, pode fornecer autenticação quando usado em um ambiente de rede confiável. Ao selecionar essa opção, insira a senha de autenticação no campo **Senha**.

   b. Caso tenha selecionado **Função hash** na lista suspensa **Autenticação**, siga estas etapas:

      1. No campo **ID de chave**, insira o hash MD5. Intervalo de valores: 1 a 255.
      2. No campo **Chave**, insira a chave MD5.

6. No campo **Custo**, insira a métrica da interface OSPF. Intervalo de valores: 1 a 65.535.
7. Na lista suspensa **Tipo de rede**, selecione o tipo de rede à qual a interface OSPF está conectada:

   - **Difusão**
   - **Não difusão**
   - **Ponto a multiponto**
   - **Ponto a ponto**

8. No campo **Prioridade**, insira a prioridade da interface OSPF. Quanto maior o valor, maior a prioridade da interface OSPF.

   A interface OSPF com prioridade mais alta se torna o roteador designado do segmento de rede. A interface OSPF com a segunda prioridade mais alta se torna o roteador designado de backup.

9. Para passar a interface OSPF para o modo passivo, marque a caixa de seleção **Interface passiva**. No modo passivo, as interfaces OSPF não trocam pacotes de tráfego.

10. Para usar o protocolo BFD para detectar a perda de conexão, marque a caixa de seleção **BFD**. Esta caixa de seleção está desmarcada por padrão.

11. Para configurar temporizadores OSPF:

    a. Marque a caixa de seleção **Temporizadores OSPF**. Esta caixa de seleção está desmarcada por padrão.

    b. No campo **Hello (s)**, insira o intervalo de tempo em segundos que a interface OSPF usa para enviar pacotes de controle a vizinhos OSPF. Intervalo de valores: 1 a 65.535.

    c. No campo **Dead (s)**, insira o intervalo de tempo em segundos que a interface OSPF usa para receber pacotes de controle de vizinhos OSPF. Se nenhum pacote de controle for recebido de um vizinho OSPF dentro do tempo especificado, a interface OSPF considera esse vizinho indisponível. Intervalo de valores: 1 a 65.535.

12. No campo **Intervalo de retransmissão (s)**, insira o intervalo de tempo em segundos para reenviar os pacotes de Anúncio de estado de link (LSA) para os vizinhos OSPF que estão atrás da interface OSPF. Intervalo de valores: 1 a 65.535. Para mais informações, consulte RFC 2328 (o parâmetro `RxmtInterval`).

13. No campo **Atraso de transmissão (s)**, insira o tempo estimado em segundos necessário para enviar um pacote LSU (Atualização de estado de link) através da interface OSPF. Intervalo de valores: 1 a 65.535. Para mais informações, consulte RFC 2328 (o parâmetro `InfTransDelay`).

14. Clique em **Criar**.

    A interface OSPF é criada e exibida na tabela.

15. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma interface OSPF

É possível editar uma interface OSPF em um modelo de CPE ou dispositivo CPE. Uma interface OSPF editada no modelo de CPE é editada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma interface OSPF:

1. Edite uma interface OSPF de uma das seguintes formas:

   - Para editar uma interface OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF → Interfaces OSPF**.

   - Para editar uma interface OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **OSPF → Interfaces OSPF** e marque a caixa de seleção **Substituir**.

   Uma tabela de interfaces OSPF é exibida.

2. Clique em **Editar** ao lado da interface OSPF que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da interface OSPF. Para obter uma descrição das configurações, consulte as instruções para criar uma interface OSPF.

4. Clique em **Salvar**.

   A interface OSPF é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma interface OSPF

É possível excluir uma interface OSPF em um modelo de CPE ou dispositivo CPE. Uma interface OSPF excluída no modelo de CPE é excluída automaticamente em todos os dispositivos CPE que usam o modelo.

As interfaces excluídas não podem ser restauradas.

Para excluir uma interface OSPF:

1. Exclua uma interface OSPF de uma das seguintes formas:

   - Para excluir uma interface OSPF em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **OSPF → Interfaces OSPF**.

   - Para excluir uma interface OSPF em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **OSPF → Interfaces OSPF** e marque a caixa de seleção **Substituir**.

   Uma tabela de interfaces OSPF é exibida.

2. Clique em **Excluir** ao lado da interface OSPF que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A interface OSPF é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Usar o BFD para detectar falhas de roteamento

O Kaspersky SD-WAN é compatível com o protocolo de detecção de encaminhamento bidirecional (BFD), que identifica problemas de conexão em links de rede em até um segundo. Quando um problema é detectado, o BFD retransmite as informações sobre o problema do plano de dados para o plano de controle.

Entre pares BFD, é estabelecida uma sessão BFD e, como parte dela, eles trocam pacotes de controle para detectar problemas de conexão de rede. Caso ocorram problemas com a conexão de rede, a sessão BFD na interface SD-WAN do dispositivo CPE é encerrada e as tabelas de rotas são então reconstruídas.

É possível visualizar a tabela de pares BFD em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de pares BFD em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BFD**.
- Para visualizar a tabela de pares BFD em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **BFD**.

As informações sobre pares BFD são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do par BFD.
- **Endereço IP** é o endereço IPv4 do par BFD.
- **Intervalo de transmissão (ms)** é o intervalo em milissegundos para o envio de pacotes de controle do dispositivo CPE ao par BFD.
- **Intervalo de recebimento (ms)** é o intervalo em milissegundos para o recebimento de pacotes de controle do par BFD no dispositivo CPE. Se nenhum pacote de controle for recebido do par BFD no tempo especificado, o dispositivo CPE considera esse par BFD indisponível.
- **Multiplicador** é o multiplicador do intervalo para o envio de pacotes de controle especificado nas configurações do par BFD. Esse multiplicador determina por quantos milissegundos o dispositivo CPE aguarda o recebimento de pacotes de controle do par BFD. Se nenhum pacote de controle for recebido do par BFD nesse período, o dispositivo CPE anuncia um problema de conexão de rede.
- **Gerenciamento** contém as ações que podem ser executadas com o par BFD.

Ativar ou desativar o protocolo BFD

É possível ativar ou desativar o protocolo BFD em um modelo de CPE ou em um dispositivo CPE. Se o protocolo BFD for ativado ou desativado em um modelo de CPE, ele é ativado ou desativado automaticamente em todos os dispositivos CPE que usam o modelo.

Para ativar ou desativar o protocolo BFD:

1. Ative ou desative o protocolo BFD de uma das seguintes formas:
   - Para ativar ou desativar o protocolo BFD em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BFD**.
   - Para ativar ou desativar o protocolo BFD em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **BFD** e marque a caixa de seleção **Substituir**.

   Uma tabela de pares BFD é exibida.

2. Na lista suspensa **BFD**, selecione um dos seguintes valores:

   - **Ativado**
   - **Desativado**. Essa é a configuração padrão.

3. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Criar um par BFD

É possível criar um par BFD em um modelo de CPE ou dispositivo CPE. Pares BFD criados no modelo de CPE são criados automaticamente em todos os dispositivos CPE que usam o modelo. Antes de criar um par BFD, ative o protocolo BFD.

Para criar um par BFD:

1. Crie um par BFD de uma das seguintes formas:

   - Para criar um par BFD em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BFD**.
   - Para criar um par BFD em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **BFD** e marque a caixa de seleção **Substituir**.

   Uma tabela de pares BFD é exibida.

2. Clique em **+ Par BFD**.

3. Na janela aberta, no campo **Nome**, insira o nome do par BFD. O comprimento máximo do nome é de 255 caracteres.

4. No campo **Endereço IP**, insira o endereço IPv4 do par BFD.

5. No campo **Intervalo de transmissão (ms)**, insira o intervalo de tempo em milissegundos para o envio de pacotes de controle do dispositivo CPE ao par BFD. Intervalo de valores: 60 a 10.000.

6. No campo **Intervalo de recebimento (ms)**, insira o intervalo de tempo em milissegundos para o recebimento de pacotes de controle do par BFD no dispositivo CPE. Se nenhum pacote de controle for recebido do par BFD no tempo especificado, o dispositivo CPE considera esse par BFD indisponível. Intervalo de valores: 60 a 10.000.

7. No campo **Multiplicador**, insira o multiplicador do intervalo de tempo para o envio de pacotes de controle especificado nas configurações do par BFD. Esse multiplicador determina por quantos milissegundos o dispositivo CPE aguarda o recebimento de pacotes de controle do par BFD. Se nenhum pacote de controle for recebido do par BFD nesse período, o dispositivo CPE anuncia um problema de conexão de rede. Intervalo de valores: 2 a 255.

   Por exemplo, caso o intervalo de tempo para o envio de pacotes de controle nas configurações de pares BFD for de 200 milissegundos e for especificado um multiplicador de 2, se após 400 milissegundos nenhum pacote de controle for recebido desse par BFD, o dispositivo CPE anuncia um problema de conectividade de rede.

8. Clique em **Criar**.

   O par BFD é criado e exibido na tabela.

9. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar um par BFD

É possível editar um par BFD em um modelo de CPE ou dispositivo CPE. Um par BFD editado no modelo de CPE é editado automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar um par BFD:

1. Edite um par BFD de uma das seguintes formas:

   - Para editar um par BFD em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BFD**.
   - Para editar um par BFD em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **BFD** e marque a caixa de seleção **Substituir**.

   Uma tabela de pares BFD é exibida.

2. Clique em **Editar** ao lado do par BFD que deseja editar.

3. Na janela aberta, se necessário, edite as configurações do par BFD. Para obter uma descrição das configurações, consulte as instruções para criar um par BFD.

4. Clique em **Salvar**.

   O par BFD é modificado e atualizado na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir um par BFD

É possível excluir um par BFD em um modelo de CPE ou dispositivo CPE. Um par BFD excluído do modelo de CPE é excluído automaticamente de todos os dispositivos CPE que usam o modelo.

Os pares BFD excluídos não podem ser restaurados.

Para excluir um par BFD:

1. Exclua um par BFD de uma das seguintes formas:

   - Para excluir um par BFD em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **BFD**.
   - Para excluir um par BFD em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **BFD** e marque a caixa de seleção **Substituir**.

   Uma tabela de pares BFD é exibida.

2. Clique em **Excluir** ao lado do par BFD que deseja excluir.

3. Na janela aberta, clique em **Excluir**.

   O par BFD é excluído e não é mais exibido na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Garantir a alta disponibilidade com o VRRP

O Kaspersky SD-WAN tem suporte para o Protocolo de Redundância de Roteador Virtual (VRRP) para combinar interfaces de rede de vários dispositivos CPE em roteadores virtuais. Quando as interfaces de rede são combinadas em um roteador virtual, elas compartilham um endereço IP virtual. Uma interface de rede é a principal e as outras são secundárias. Um endereço IP virtual é atribuído à interface de rede principal.

As interfaces de rede em um roteador virtual trocam pacotes de controle para determinar quais interfaces de rede falharam. Se a interface de rede principal falhar, uma nova interface de rede principal será escolhida e um endereço IP virtual é atribuído a ela. O tráfego retransmitido para o endereço IP virtual através da interface de rede com falha é automaticamente assumido pela nova interface de rede principal.

É possível criar instâncias de VRRP para combinar interfaces de rede em um roteador virtual. Ao criar uma instância VRRP, especifique uma interface de rede, um ID de Roteador Virtual (VRID) e um endereço IP virtual. As interfaces de rede são combinadas em um roteador virtual quando o mesmo ID de roteador virtual e o mesmo endereço IP virtual são especificados nas instâncias VRRP criadas para elas.

Para alterar de forma síncrona a interface de rede principal em vários roteadores virtuais, crie grupos de instâncias VRRP. Se a interface de rede principal for alterada em uma das instâncias VRRP, essa alteração também ocorre em todas as outras instâncias VRRP no grupo de instâncias VRRP.

Ativar ou desativar o protocolo VRRP

É possível ativar ou desativar o protocolo VRRP em um modelo de CPE ou em um dispositivo CPE. Se o protocolo VRRP for ativado ou desativado em um modelo de CPE, ele é ativado ou desativado automaticamente em todos os dispositivos CPE que usam o modelo.

Para ativar ou desativar o protocolo VRRP:

1. Ative ou desative o protocolo VRRP de uma das seguintes formas:

   - Para ativar ou desativar o protocolo VRRP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRRP → Instâncias VRRP**.

   - Para ativar ou desativar o protocolo VRRP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **VRRP → Instâncias VRRP** e marque a caixa de seleção **Substituir**.

   Uma tabela de instâncias VRPP é exibida.

2. Na lista suspensa **VRRP**, selecione um dos seguintes valores:

   - **Ativado**

   - **Desativado**. Essa é a configuração padrão.

   Ao ativar o VRRP, é necessário criar pelo menos uma instância VRRP.

3. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar instâncias VRRP

É possível visualizar a tabela de instâncias VRRP em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de instâncias VRRP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Instâncias VRRP → VRRP**.

- Para visualizar a tabela de instâncias VRRP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **VRRP → Instâncias VRRP**.

As informações sobre instâncias VRRP são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da instância VRRP.

- **VRID** é o ID do roteador virtual.

- **Interface** é a interface de rede que foi adicionada ao roteador virtual.

- **VIP** é o endereço IP virtual atribuído à interface de rede.

- **Estado** é a função da interface de rede:

  - **Backup** é a interface de rede de backup.

  - **Principal** é a interface de rede principal.

- **Prioridade** é a prioridade da interface de rede. Quanto maior o valor, maior a prioridade. Quando a interface de rede principal falha, ela é substituída pela interface de rede de backup com a prioridade mais alta. Se, ao selecionar a nova interface de rede principal, todas as interfaces de rede de backup tiverem a mesma prioridade, a nova interface de rede principal é selecionada aleatoriamente.
- **Intervalo de anúncio (s)** é o intervalo de tempo, em segundos, para enviar pacotes de controle de uma interface de rede para outras interfaces de rede.
- **Nopreempt** especifica se a função da interface de rede que se tornou a principal deve ser alterada se a interface de rede principal anterior for recuperada:
  - **Sim**.
  - **Não**.
- **Gerenciamento** contém as ações que podem ser executadas com a instância VRRP.

Criar uma instância VRRP

É possível criar uma instância VRRP em um modelo de CPE ou em um dispositivo CPE. Instâncias VRRP criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma instância VRRP:

1. Crie uma instância VRRP de uma das seguintes formas:
   - Para criar uma instância VRRP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRRP → Instâncias VRRP**.
   - Para criar uma instância VRRP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **VRRP → Instâncias VRRP** e marque a caixa de seleção **Substituir**.

   Uma tabela de instâncias VRPP é exibida.
2. Clique em **+ Instância VRRP**.
3. Na janela aberta, no campo **Nome**, insira o nome da instância VRRP. O comprimento máximo do nome é de 16 caracteres.
4. No campo **VRID**, insira o ID do roteador virtual. Especifique o mesmo ID ao criar instâncias VRRP para todas as interfaces de rede que deseja combinar em um roteador virtual. Intervalo de valores: 1 a 255.
5. Na lista suspensa **Interface**, selecione a interface de rede criada que deseja adicionar ao roteador virtual.
6. No campo **VIP**, insira o endereço IP virtual que deseja atribuir à interface de rede. É necessário atribuir o mesmo endereço IP virtual a todas as interfaces de rede que deseja combinar em um roteador virtual.
7. Na lista suspensa **Estado**, selecione a função da interface de rede:
   - **Backup** é a interface de rede de backup. Essa é a configuração padrão.
   - **Principal** é a interface de rede principal.

8. No campo **Prioridade**, insira a prioridade da interface de rede. Quanto maior o valor, maior a prioridade. Quando a interface de rede principal falha, ela é substituída pela interface de rede de backup com a prioridade mais alta. Se, ao selecionar a nova interface de rede principal, todas as interfaces de rede de backup tiverem a mesma prioridade, a nova interface de rede principal é selecionada aleatoriamente. Intervalo de valores: 1 a 255. O valor padrão é `100`.

9. No campo **Intervalo de anúncio (s)**, insira o intervalo de tempo, em segundos, para enviar pacotes de controle de uma interface de rede para outras interfaces de rede. Intervalo de valores: 1 a 60. O valor padrão é `5`.

10. Caso não deseje alterar a função da interface de rede de backup que se tornou o roteador principal, mesmo que a interface de rede principal antiga fique operacional novamente, marque a caixa de seleção **Nopreempt**. Esta caixa de seleção está desmarcada por padrão.

11. Para configurar o envio unicast de pacotes de controle pela interface de rede:

    a. Marque a caixa de seleção **Unicast**. Esta caixa de seleção está desmarcada por padrão.

    b. No campo **IP de origem do unicast**, insira o endereço IP da interface de rede de origem para enviar pacotes de controle.

    c. No campo **IP de par do unicast**, insira o endereço IP da interface de rede de destino para enviar pacotes de controle.

    Por padrão, a interface de rede usa multicast para enviar pacotes de controle.

12. Para usar uma senha para autenticação de pacotes de controle na interface de rede:

    a. Marque a caixa de seleção **Autenticação**. Esta caixa de seleção está desmarcada por padrão.

    b. Insira uma senha no campo exibido. O comprimento máximo da senha é de 16 caracteres. Especifique a mesma senha para todas as interfaces de rede que deseja combinar em um roteador virtual. Para ver a senha inserida, clique no ícone de exibição 👁.

13. Clique em **Criar**.

    A instância VRRP é criada e exibida na tabela.

14. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma instância VRRP

É possível editar uma instância VRRP em um modelo de CPE ou em um dispositivo CPE. Uma instância VRRP editada no modelo de CPE é editada automaticamente em todos os dispositivos CPE que usam o modelo. Não é possível editar uma instância VRRP herdada de um modelo de CPE em um dispositivo CPE.

Para editar uma instância VRRP:

1. Edite uma instância VRRP de uma das seguintes formas:

   - Para editar uma instância VRRP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRRP → Instâncias VRRP**.

   - Para editar uma instância VRRP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **VRRP → Instâncias VRRP** e marque a caixa de seleção **Substituir**.

   Uma tabela de instâncias VRPP é exibida.

2. Clique em **Editar** ao lado da instância VRRP que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da instância VRRP. Para obter uma descrição das configurações, consulte as instruções para criar uma instância VRRP.

4. Clique em **Salvar**.

   A instância VRRP é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma instância VRRP

É possível excluir uma instância VRRP em um modelo de CPE ou em um dispositivo CPE. Uma instância VRRP excluída do modelo de CPE é excluída automaticamente de todos os dispositivos CPE que usam o modelo. Não é possível excluir uma instância VRRP herdada de um modelo de CPE em um dispositivo CPE.

As instâncias VRRP excluídas não podem ser restauradas.

Para excluir uma instância VRRP:

1. Exclua uma instância VRRP de uma das seguintes formas:

   - Para excluir uma instância VRRP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRRP → Instâncias VRRP**.

   - Para excluir uma instância VRRP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **VRRP → Instâncias VRRP** e marque a caixa de seleção **Substituir**.

   Uma tabela de instâncias VRPP é exibida.

2. Clique em **Excluir** ao lado da instância VRRP que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A instância VRRP é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar grupos de instâncias VRRP

É possível visualizar a tabela de grupos de instâncias VRRP em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de grupos de instâncias VRRP em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRRP** → **Grupos de instâncias VRRP**.
- Para visualizar a tabela de grupos de instâncias VRRP em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **VRRP** → **Grupos de instâncias VRRP**.

As informações sobre grupos de instâncias VRRP são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do grupo de instâncias VRRP.
- **Instâncias VRRP** são as instâncias VRRP que foram adicionadas ao grupo de instâncias VRRP.
- **Gerenciamento** contém as ações que podem ser executadas com o grupo de instâncias VRRP.

Criar um grupo de instâncias VRRP

É possível criar um grupo de instâncias VRRP em um modelo de CPE ou em um dispositivo CPE. Grupos de instâncias VRRP criados no modelo de CPE são criados automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar um grupo de instâncias VRRP:

1. Crie um grupo de instâncias VRRP de uma das seguintes formas:

   - Para criar um grupo de instâncias VRRP em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRRP** → **Grupos de instâncias VRRP**.
   - Para criar um grupo de instâncias VRRP em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **VRRP** → **Grupos de instâncias VRRP** e marque a caixa de seleção **Substituir**.

   Uma tabela de grupos de instâncias VRRP é exibida.

2. Clique em **+ Grupo de instâncias VRRP**.
3. Na janela aberta, no campo **Nome**, insira o nome do grupo de instâncias VRRP. O comprimento máximo do nome é de 16 caracteres. O valor padrão é `1`.
4. Na lista suspensa **Instâncias VRRP**, selecione a instância VRRP criada que deseja adicionar ao grupo de instâncias VRRP.

   A instância VRRP é adicionada e exibida na parte inferior da janela. É possível adicionar várias instâncias VRRP ou excluir instâncias VRRP. Para excluir uma instância VRRP, clique em **Excluir** ao lado dela.

5. Clique em **Criar**.

   O grupo de instâncias VRRP é criado e exibido na tabela.

6. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar um grupo de instâncias VRRP

É possível editar um grupo de instâncias VRRP em um modelo de CPE ou em um dispositivo CPE. Um grupo de instâncias VRRP editado no modelo de CPE é editado automaticamente em todos os dispositivos CPE que usam o modelo. Não é possível editar um grupo de instâncias VRRP herdado de um modelo de CPE em um dispositivo CPE.

Para editar um grupo de instâncias VRRP:

1. Edite um grupo de instâncias VRRP de uma das seguintes formas:

   - Para editar um grupo de instâncias VRRP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRRP → Grupos de instâncias VRRP**.
   - Para editar um grupo de instâncias VRRP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **VRRP → Grupos de instâncias VRRP** e marque a caixa de seleção **Substituir**.

   Uma tabela de grupos de instâncias VRRP é exibida.

2. Clique em **Editar** ao lado do grupo de instâncias VRRP que deseja editar.

3. Na janela aberta, se necessário, edite o nome do grupo de instâncias VRRP e adicione ou exclua instâncias VRRP criadas.

4. Clique em **Salvar**.

   O grupo de instâncias VRRP é modificado e atualizado na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir um grupo de instâncias VRRP

É possível excluir um grupo de instâncias VRRP em um modelo de CPE ou em um dispositivo CPE. Um grupo de instâncias VRRP excluído do modelo de CPE é excluído automaticamente de todos os dispositivos CPE que usam o modelo. Não é possível excluir um grupo de instâncias VRRP herdado de um modelo de CPE em um dispositivo CPE.

Os grupos de instâncias VRRP excluídos não podem ser restaurados.

Para excluir um grupo de instâncias VRRP:

1. Exclua um grupo de instâncias VRRP de uma das seguintes formas:

   - Para excluir um grupo de instâncias VRRP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRRP → Grupos de instâncias VRRP**.

   - Para excluir um grupo de instâncias VRRP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **VRRP → Grupos de instâncias VRRP** e marque a caixa de seleção **Substituir**.

   Uma tabela de grupos de instâncias VRRP é exibida.

2. Clique em **Excluir** ao lado do grupo de instâncias VRRP que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   O grupo de instâncias VRRP é excluído e não é mais exibido na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Transmissão de tráfego multicast usando os protocolos PIM e IGMP

O Kaspersky SD-WAN é compatível com a transmissão de tráfego multicast entre dispositivos CPE e dispositivos de rede externos usando os protocolos PIM e IGMP. É possível especificar as configurações básicas do protocolo PIM em dispositivos CPE, por exemplo, os pontos de encontro a serem usados, e, em seguida, criar interfaces multicast para interação com outros dispositivos CPE. As interfaces de rede criadas são usadas como interfaces multicast.

Se a conexão PIM for estabelecida entre dispositivos CPE e os pontos de encontro forem definidos para esses dispositivos, as interfaces multicast podem receber solicitações IGMP de clientes por meio de IGMP. As solicitações IGMP contêm endereços IP de fontes das quais os clientes desejam receber pacotes de tráfego multicast. Quando as fontes enviam pacotes multicast para um ponto de encontro, os clientes recebem esses pacotes de tráfego multicast.

Se necessário, use o protocolo PIM para conectar dispositivos CPE a roteadores externos. Parar isso, ative o protocolo PIM na interface multicast à qual o roteador externo está conectado.

Configurações básicas de PIM

É possível especificar configurações básicas de PIM em um modelo de CPE ou no dispositivo CPE. As configurações básicas de PIM especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para modificar as configurações básicas de PIM:

1. Especifique as configurações básicas de PIM de uma das seguintes formas:

   - Para editar as configurações básicas de PIM em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Multicast**.

   - Para editar as configurações básicas de PIM em dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Multicast**.

   Por padrão, é selecionada a guia **Configurações gerais**, que exibe as configurações básicas de PIM.

2. Na lista suspensa **Multicast**, selecione **Ativado**. O valor padrão é **Desativado**.

3. Especifique o ponto de encontro para fontes de pacotes de tráfego multicast e clientes conectados ao dispositivo CPE:

   a. Em **IP do RP**, clique em **+ Adicionar** e insira o endereço IPv4 do ponto de encontro.

   b. Para especificar um grupo multicast associado ao ponto de encontro, em **Grupo RP**, insira o prefixo IPv4 do grupo multicast. Cada ponto de encontro pode ser associado a um grupo multicast dedicado.

   O ponto de encontro é especificado e exibido nas seções **IP do RP** e **Grupo RP**. É possível especificar vários pontos de encontro ou excluir pontos de encontro. Para excluir um ponto de encontro, clique no ícone de exclusão ✕ ao lado dele.

4. No campo **Temporizador keepalive RP (s)**, insira o tempo de vida, em segundos, dos fluxos de tráfego entre a origem e o grupo multicast (S,G). A contagem é reiniciada se o dispositivo CPE receber um pacote de registro. Intervalo de valores: 31 a 60.000. O valor padrão é `185`.

5. Para filtrar pacotes de tráfego multicast com os endereços IPv4 de origem especificados no dispositivo CPE, na lista suspensa **Lista de aceitação de registro PIM**, selecione uma lista de prefixos criada.

6. Se um dispositivo CPE estiver no último salto e você quiser impedir que esse dispositivo CPE mude da árvore compartilhada para a árvore de caminho mais curto (SPT) ao transmitir pacotes de tráfego multicast:

   a. Marque a caixa de seleção **Alternância de SPT**. Esta caixa de seleção está desmarcada por padrão.

   b. Para negar ou permitir a mudança da Árvore de Ponto de Encontro (RPT) para a árvore de caminho mais curto ao transmitir pacotes de tráfego de grupos multicast com prefixos IPv4 de origem especificados, selecione uma lista de prefixos criada na lista suspensa **Lista de prefixos SPT**. Se a mudança é negada ou permitida é determinado da seguinte forma:

      - Se a lista de prefixos permitir o prefixo IPv4, a mudança não ocorre.

      - Se a lista de prefixos negar o prefixo IPv4, a mudança ocorre.

7. Para executar o balanceamento ECMP em um dispositivo CPE para distribuir fluxos de tráfego multicast por várias rotas:

    a. Marque a caixa de seleção **ECMP**. Esta caixa de seleção está desmarcada por padrão. Para o balanceamento ECMP, diversas rotas devem existir. Se o balanceamento ECMP estiver desativado, o tráfego será transmitido ao longo de uma rota.

    b. Para equilibrar todo o tráfego entre as rotas restantes caso uma das interfaces multicast falhe, marque a caixa de seleção **Rebalanceamento de ECMP**. A caixa de seleção está desmarcada por padrão e, se uma das interfaces multicast falhar, apenas o tráfego transmitido por meio dessa interface multicast será redistribuído.

8. No campo **Intervalo PIM join/prune (s)**, insira o tempo, em segundos, para que as interfaces multicast enviem pacotes join/prune aos pares PIM. Intervalo de valores: 60 a 600. O valor padrão é `60`.

9. No campo **Temporizador keepalive PIM (s)**, insira o tempo de vida, em segundos, dos fluxos de tráfego entre a origem e o grupo multicast (S,G). A contagem é reiniciada se o dispositivo CPE receber um pacote join/prune. Intervalo de valores: 31 a 60.000. O valor padrão é `210`.

10. Para que o dispositivo CPE retransmita pacotes de tráfego com prefixos IPv4 de origem especificados de grupos multicast mediante solicitação do cliente (Multicast específico da origem; SSM), na lista suspensa **Lista de prefixos SSM**, selecione uma lista de prefixos criada.

11. Na lista suspensa **Modo de pesquisa RPF**, selecione um modo de pesquisa de Encaminhamento de caminho reverso (RPF) no dispositivo CPE:

    - **longer-prefix**.
    - **lower-distance**.
    - **mrib-only**.
    - **mrib-then-urib**. Essa é a configuração padrão.
    - **urib-only**.

12. Para adicionar uma rota IPv4 estática à tabela de roteamento multicast do dispositivo CPE:

    a. Em **Rotas multicast estáticas**, clique em **+ Adicionar**.

    b. No campo **IP do destino**, insira o endereço IPv4 de destino da rota estática.

    c. Na lista suspensa **Tipo**, selecione o tipo de origem da rota estática:

        - **Endereço** é um endereço IPv4. Ao selecionar esse valor, no campo **Nexthop**, insira o endereço IPv4 de origem e o prefixo da rota estática.
        - **Interface** é a interface de rede criada. Ao selecionar esse valor, na lista suspensa **Nexthop**, selecione a interface de rede de origem da rota estática.

    d. Se necessário, no campo **Distância**, insira a métrica da rota estática. Intervalo de valores: 1 a 255.

A rota estática é adicionada e exibida em **Rotas multicast estáticas**. É possível adicionar várias rotas estáticas ou excluir rotas estáticas. Para excluir uma rota estática, clique no ícone de exclusão ✕ ao lado dela.

13. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar interfaces multicast

É possível visualizar a tabela de interfaces multicast em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de interfaces multicast em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Multicast → Interfaces**.
- Para visualizar a tabela de interfaces multicast em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Multicast → Interfaces**.

As informações sobre as interfaces multicast são exibidas nas seguintes colunas da tabela:

- **Interface de rede** é a interface de rede usada como interface multicast.
- **PIM** indica se a troca de mensagens com pares através do protocolo PIM está ativada na interface multicast:
  - **Ativado**
  - **Desativado**
- **IGMP** indica se a troca de mensagens com pares através do protocolo IGMP está ativada na interface multicast:
  - **Ativado**
  - **Desativado**
- **Prioridade do DR** é a prioridade da interface multicast. A interface multicast com prioridade mais alta se torna o roteador designado do segmento de LAN. Quanto maior o valor, maior a prioridade da interface multicast.
- **Herdado** indica se a interface multicast é herdada de um modelo de CPE:
  - **Sim**.
  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.
- **Gerenciamento** contém as ações que podem ser executadas com a interface multicast.

Criar uma interface multicast

É possível criar uma interface multicast em um modelo de CPE ou em um único dispositivo. Interfaces multicast criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma interface multicast:

1. Crie uma interface multicast de uma das seguintes formas:

   - Para criar uma interface multicast em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Multicast → Interfaces**.
   - Para criar uma interface multicast em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Multicast → Interfaces** e marque a caixa de seleção **Substituir**.

   Uma tabela de interfaces multicast é exibida.

2. Clique em **+ interface multicast**.
3. Na janela aberta, na lista suspensa **Interface de rede**, selecione uma interface de rede criada que deseja usar como interface multicast.
4. Configure o protocolo PIM na interface multicast:
   a. Na lista suspensa **PIM**, selecione **Ativado**. O valor padrão é **Desativado**.
   b. Para passar a interface multicast para o modo passivo, marque a caixa de seleção **Passiva**. No modo passivo, as interfaces multicast não trocam pacotes de controle. Esta caixa de seleção está desmarcada por padrão.
   c. Para proibir a troca de pacotes bootstrap na interface multicast, desmarque a caixa de seleção **BSM**. Esta caixa de seleção é selecionada por padrão.
   d. Para proibir a troca de pacotes bootstrap unicast na interface multicast, desmarque a caixa de seleção **BSM unicast**. Esta caixa de seleção é selecionada por padrão.
   e. No campo **Prioridade do DR**, insira a prioridade da interface multicast. A interface multicast com prioridade mais alta se torna o roteador designado do segmento de LAN. Quanto maior o valor, maior a prioridade da interface multicast. Intervalo de valores: 1 a 4.294.967.295. O valor padrão é `1`.
   f. No campo **Hello (s)**, insira o intervalo de tempo em segundos que a interface multicast usa para enviar pacotes de controle a vizinhos PIM. Intervalo de valores: 1 a 180. O valor padrão é `30`.
   g. No campo **Reter (s)**, insira o intervalo de tempo em segundos que a interface multicast usa para receber pacotes de controle de vizinhos PIM. Se nenhum pacote de controle for recebido de um vizinho PIM dentro do tempo especificado, a interface PIM considera esse vizinho indisponível. Intervalo de valores: 1 a 630. O valor padrão é `105`.
   h. Se vários endereços IP forem atribuídos a uma interface multicast e você quiser usar o endereço IPv4 de origem especificado ao enviar mensagens PIM, insira o endereço IPv4 no campo **IP de origem**.
5. Configure o protocolo IGMP na interface multicast:
   a. Na lista suspensa **IGMP**, selecione **Ativado**. O valor padrão é **Desativado**.
   b. Na lista suspensa **Versão**, selecione a versão do protocolo IGMP na interface multicast:
      - **2**.
      - **3**. Essa é a configuração padrão.

c. No campo **Intervalo entre consultas (s)**, insira o intervalo de tempo em segundos para o envio de consultas da interface multicast a clientes. As consultas são usadas para determinar se o tráfego multicast precisa ser enviado aos clientes. Intervalo de valores: 1 a 250. O valor padrão é `125`.

d. No campo **Tempo de resposta de consulta (s)**, insira o tempo em segundos que a interface multicast deve esperar para receber respostas dos clientes. Se nenhuma resposta a uma consulta for recebida do cliente no tempo especificado, a interface multicast não enviará pacotes de tráfego. Intervalo de valores: 1 a 125. O valor padrão é `10`.

e. Para especificar grupos multicast:

1. Em **Ingressar no grupo**, clique em **+ Adicionar** e insira o endereço IPv4 do grupo multicast.

2. Para conectar a interface multicast à fonte especificada do grupo multicast, em **Endereço da fonte**, insira o endereço IPv4 da origem.

O grupo multicast é especificado e exibido nas seções **Ingressar no grupo** e **Endereço da fonte**. É possível especificar vários grupos multicast ou excluir grupos multicast. Para excluir um grupo multicast, clique no ícone de exclusão ✕ ao lado dele.

É necessário especificar grupos multicast em um dos seguintes casos:

- O segmento de rede tem clientes permanentes para os quais é necessário enviar pacotes de tráfego de um grupo multicast de forma rápida e estável.

- O segmento de rede não contém clientes ou os hosts no segmento não podem enviar mensagens de relatório, mas os pacotes de tráfego de um grupo multicast devem ser enviados para esse segmento.

6. Clique em **Criar**.

A interface multicast é criada e exibida na tabela.

7. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Editar uma interface multicast

É possível editar as configurações da interface multicast em um modelo de CPE ou em um dispositivo CPE. Uma interface multicast editada no modelo de CPE é editada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma interface multicast:

1. Edite a interface multicast de uma das seguintes formas:

- Para editar uma interface multicast em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Multicast → Interfaces**.

- Para editar uma interface multicast em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Multicast → Interfaces** e marque a caixa de seleção **Substituir**.

Uma tabela de interfaces multicast é exibida.

2. Clique em **Editar** ao lado da interface multicast que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da interface multicast. Para obter uma descrição das configurações, consulte as instruções para criar uma interface multicast.

4. Clique em **Salvar**.

   A interface multicast é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma interface multicast

É possível excluir uma interface multicast em um modelo de CPE ou dispositivo CPE. Uma interface multicast excluída no modelo de CPE é excluída automaticamente em todos os dispositivos CPE que usam o modelo.

As interfaces multicast excluídas não podem ser restauradas.

Para excluir uma interface multicast:

1. Exclua a interface multicast de uma das seguintes formas:

   - Para excluir uma interface multicast em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Multicast → Interfaces**.

   - Para excluir uma interface multicast em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Multicast → Interfaces** e marque a caixa de seleção **Substituir**.

   Uma tabela de interfaces multicast é exibida.

2. Clique em **Excluir** ao lado da interface multicast que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A interface multicast é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Gerenciar tabelas de roteamento e encaminhamento virtual (VRF)

O Kaspersky SD-WAN é compatível com a tecnologia de roteamento e encaminhamento virtual (VRF) para a criação de tabelas de roteamento e encaminhamento virtual em dispositivos CPE. É possível criar até 100 tabelas de roteamento e encaminhamento virtual.

Ao criar uma tabela de roteamento e encaminhamento virtual, selecione as interfaces de rede que deseja adicionar a ela. Não é possível adicionar a mesma interface de rede a múltiplas tabelas de roteamento e encaminhamento virtual. As interfaces de rede para conectar o dispositivo CPE ao controlador e ao orquestrador são automaticamente adicionadas à tabela de roteamento e encaminhamento virtual padrão e não é possível adicioná-las a outras tabelas.

Se as interfaces de rede forem adicionadas a tabelas de roteamento e encaminhamento virtual diferentes, as redes conectadas a essas interfaces não terão acesso umas às outras. Nessa situação, as interfaces de rede podem ter endereços IP de sub-redes idênticas ou sobrepostas.

Ao criar uma tabela de roteamento e encaminhamento virtual, uma interface de rede do sistema correspondente a essa tabela é criada automaticamente no dispositivo CPE. Essa interface de rede do sistema é usada para encaminhar tráfego entre interfaces de rede na tabela de roteamento e encaminhamento virtual. Para que a interface de rede do sistema funcione, crie um registro para ela na interface da Web do orquestrador.

Ao criar uma tabela de roteamento e encaminhamento virtual, é possível criar uma rota blackhole para isolar o tráfego. Nesse caso, a rota blackhole 0.0.0.0/0 é criada automaticamente no dispositivo e as informações sobre ela são exibidas na seção **Rotas estáticas**. Sem uma rota blackhole, o tráfego pode acabar em outras tabelas de roteamento e encaminhamento virtual.

Se nenhuma zona de firewall for atribuída às interfaces de rede na tabela de roteamento e encaminhamento virtual, é necessário assegurar-se de que, por padrão, o firewall do dispositivo CPE aceita pacotes de tráfego encaminhados entre interfaces de rede e sub-redes. É possível especificar ações padrão ao definir as configurações básicas do firewall.

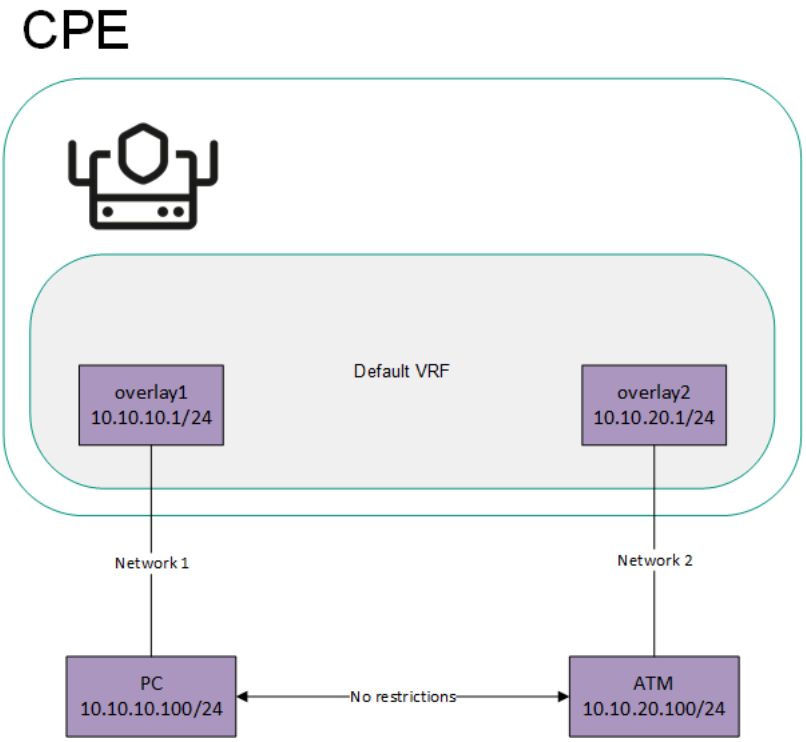
Se as zonas de firewall forem atribuídas a interfaces de rede na tabela de roteamento e encaminhamento virtual e o firewall do dispositivo CPE não aceitar por padrão pacotes de tráfego encaminhados entre interfaces de rede e sub-redes, será necessário atribuir uma zona de firewall à interface de rede do sistema. A zona de firewall atribuída também deve ser atribuída a uma das interfaces de rede na tabela de roteamento e encaminhamento virtual.

É possível adicionar rotas BGP e rotas estáticas às tabelas de roteamento e encaminhamento virtual de um dispositivo CPE. Para adicionar rotas BGP a uma tabela de roteamento e encaminhamento virtual, especifique a tabela ao editar as configurações básicas do BGP. Para adicionar uma rota estática a uma tabela de roteamento e encaminhamento virtual, especifique a tabela ao adicionar a rota estática.

As tabelas de roteamento e encaminhamento virtual podem ser usadas nos seguintes cenários:

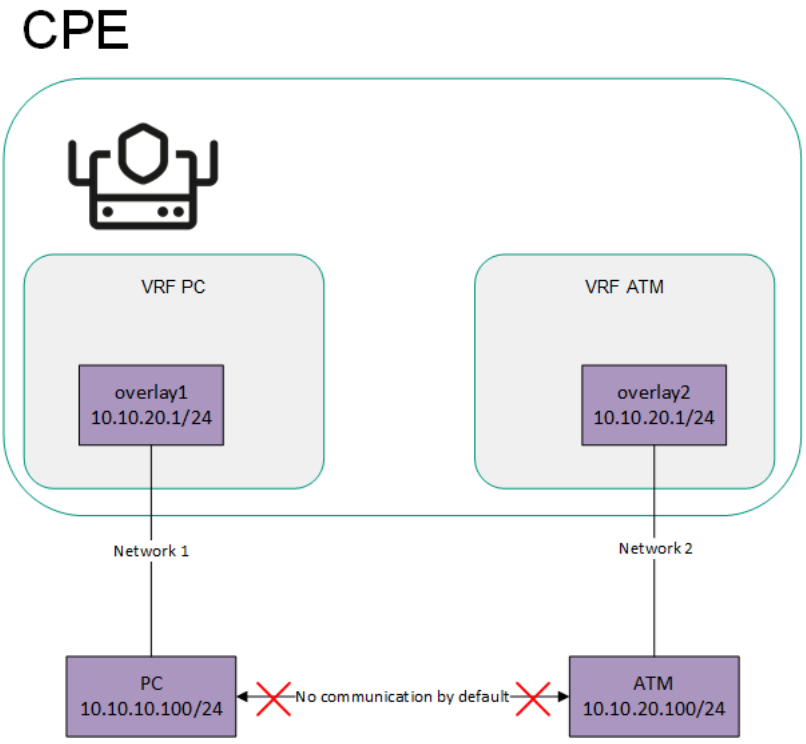
- **Segmentação de rede usando tabelas de roteamento e encaminhamento virtual**

  É possível criar tabelas de roteamento e encaminhamento virtual para segmentar sua rede. Na figura abaixo, a rede 1 está construída entre a interface de rede 'overlay1' e os PCs de usuário, e a rede 2 entre a interface de rede 'overlay2' e os caixas eletrônicos. Ambas as interfaces de rede estão na tabela de roteamento e encaminhamento virtual padrão (VRF padrão), assim, as redes têm acesso uma à outra e ficam inseguras.



Interfaces de rede conectadas a redes diferentes na tabela de roteamento e encaminhamento virtual padrão

Para isolar as redes 1 e 2, as interfaces de rede overlay1 e overlay2 devem ser adicionadas a diferentes tabelas de roteamento e encaminhamento virtual (VRF PC e VRF ATM), o que cria dois segmentos (veja a figura abaixo).

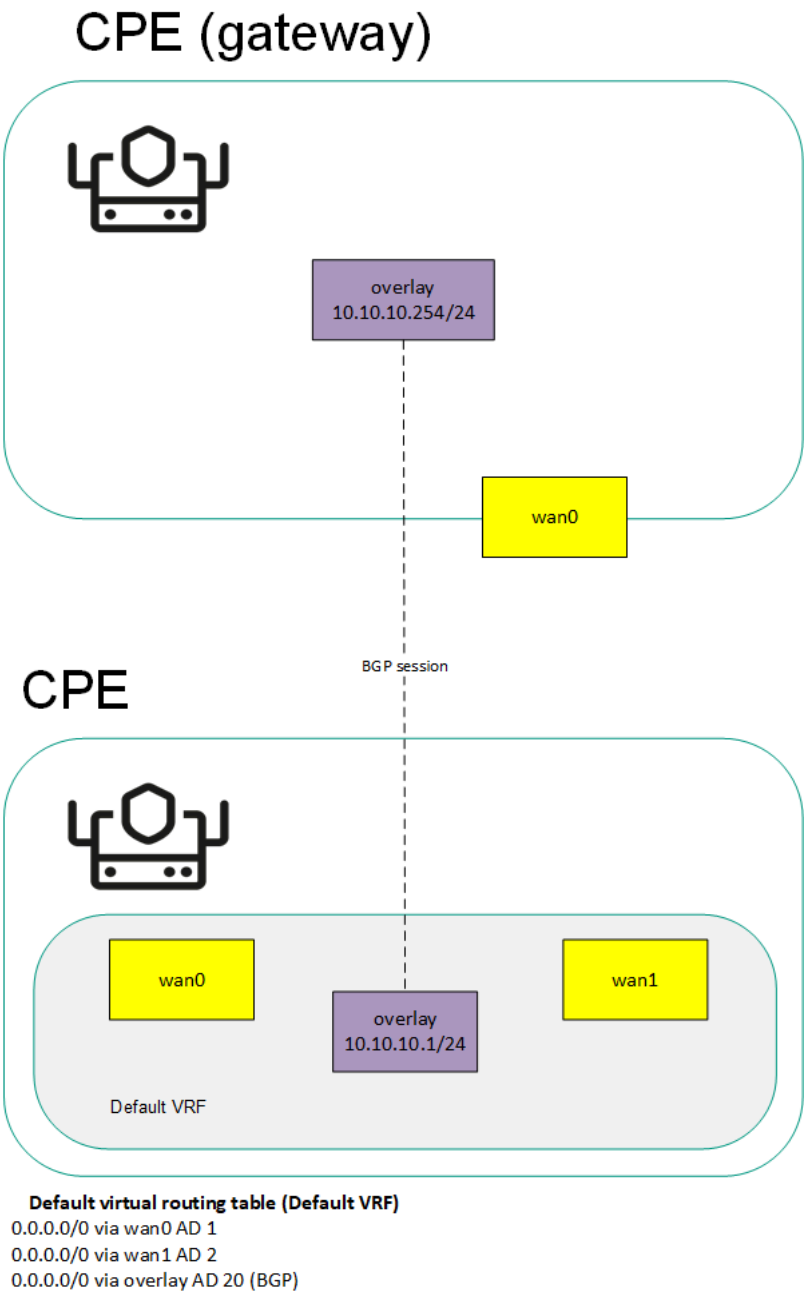


As interfaces de rede conectadas a redes diferentes estão em tabelas de roteamento e encaminhamento virtual padrão separadas

- **Enviar 0.0.0.0/0 por BGP**.

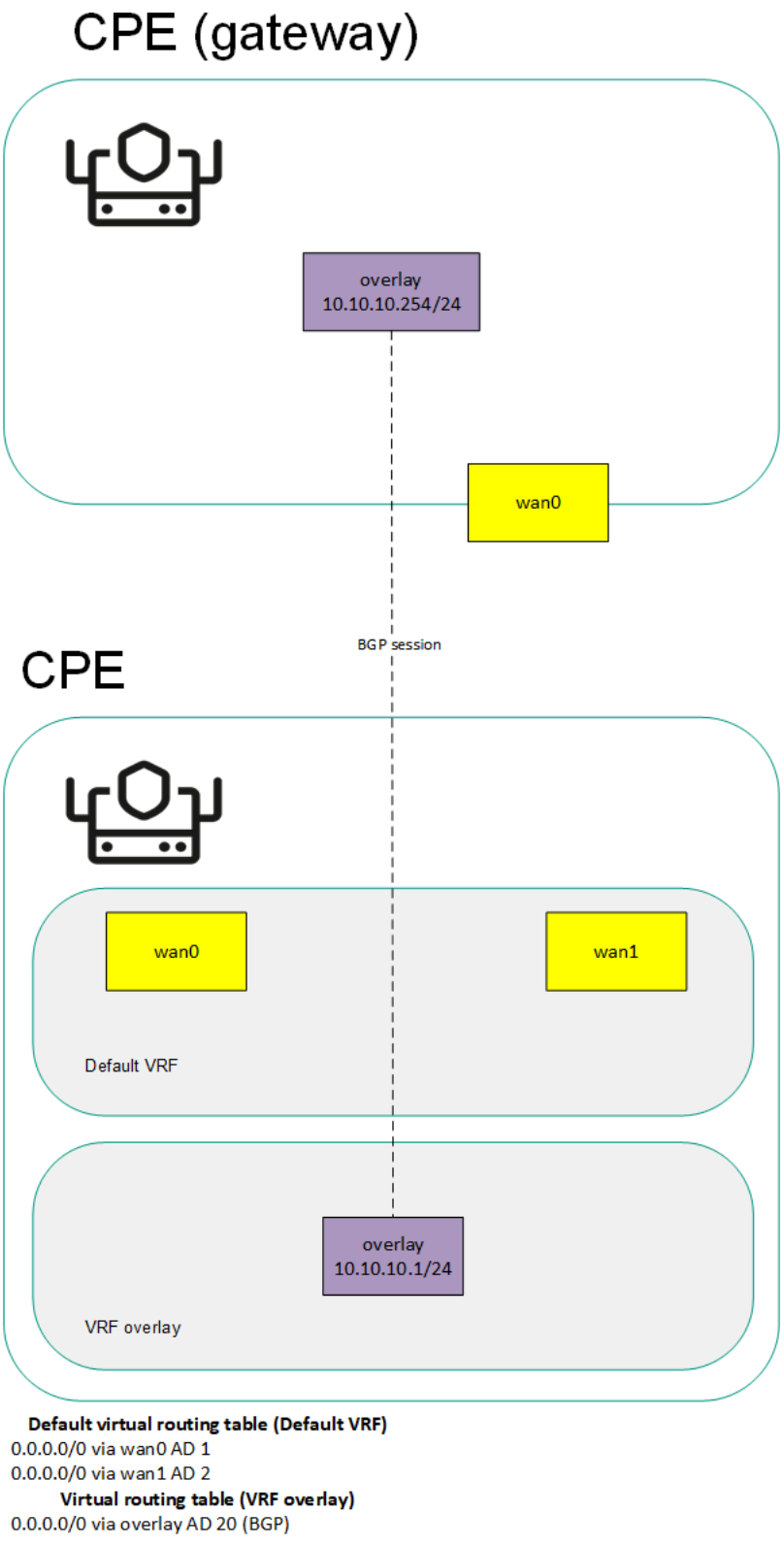
  É possível criar uma tabela de roteamento e encaminhamento virtual separada para enviar a rota 0.0.0.0/0 entre dispositivos por BGP. A figura abaixo mostra um dispositivo CPE com a função de gateway SD-WAN e um dispositivo CPE padrão. Todas as interfaces de rede do dispositivo CPE são adicionadas à tabela de roteamento e encaminhamento virtual padrão (VRF padrão).

Se o gateway SD-WAN enviar a rota BGP 0.0.0.0/0 da interface de rede overlay 10.10.10.254/24 para a interface de rede overlay 10.10.10.1/24, essa rota não poderá ser usada. Isso acontece porque a tabela de roteamento e encaminhamento virtual padrão já tem rotas 0.0.0.0/0 com uma distância administrativa mais baixa para estabelecer conexão com o controlador e o orquestrador.



Enviar a rota 0.0.0.0/0 para um dispositivo CPE com a tabela de roteamento e encaminhamento virtual padrão

Para enviar a rota 0.0.0.0/0 por BGP pela interface de rede overlay 10.10.10.254/24 para a overlay 10.10.10.1/24, crie uma tabela de roteamento e encaminhamento virtual (VRF overlay) separada para a interface de rede overlay 10.10.10.1/24 e adicione rotas BGP a ela (veja a figura abaixo).



Enviar a rota 0.0.0.0/0 para um dispositivo CPE com uma tabela de roteamento e encaminhamento virtual separada para rotas BGP

Para visualizar a tabela de tabelas de roteamento e encaminhamento virtual em um modelo de CPE e em um dispositivo CPE:

- Para visualizar a tabela de tabelas de roteamento e encaminhamento virtual em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRF**.
- Para visualizar a tabela de tabelas de roteamento e encaminhamento virtual em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **VRF**.

As informações sobre tabelas de roteamento e encaminhamento virtual são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da tabela de roteamento e encaminhamento virtual.
- **Herdado** indica se a tabela de roteamento e encaminhamento virtual foi herdada do modelo de CPE:
  - **Sim**.
  - **Não**.

  Essa coluna é exibida apenas no dispositivo CPE.
- **Tabela** é o ID da tabela de roteamento e encaminhamento virtual.
- **Interfaces** são interfaces de rede adicionadas à tabela de roteamento e encaminhamento virtual.

Especificar configurações principais relacionadas a tabelas de roteamento e encaminhamento virtual

É possível especificar configurações de kernel relacionadas a tabelas de roteamento e encaminhamento virtual em um modelo de CPE ou em um dispositivo CPE. Isso é necessário para a operação correta dos serviços de rede nas tabelas de roteamento e encaminhamento virtual criadas. As configurações de kernel especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para especificar as configurações de kernel:

1. Especifique as configurações de kernel de uma das seguintes formas:
   - Para editar as configurações de kernel em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRF** → **Configurações gerais**.
   - Para editar as configurações de kernel em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **VRF** → **Configurações gerais** e marque a caixa de seleção **Substituir**.

   As configurações de kernel são exibidas.

2. Se necessário, execute uma das seguintes ações:

   - Para usar os serviços de rede UDP no roteamento e encaminhamento virtual, marque a caixa de seleção **Serviços de rede UDP em todos os VRFs**. Esta caixa de seleção está desmarcada por padrão.
   - Para usar os serviços de rede TCP no roteamento e encaminhamento virtual, marque a caixa de seleção **Serviços de rede TCP em todos os VRFs**. Esta caixa de seleção está desmarcada por padrão.
   - Caso não queira usar soquetes brutos no roteamento e encaminhamento virtual, desmarque a caixa de seleção **Soquetes brutos em todos os VRFs**. Esta caixa de seleção é selecionada por padrão.

3. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Criar uma tabela de roteamento e encaminhamento virtual

É possível criar uma tabela de roteamento e encaminhamento virtual em um modelo de CPE ou em um dispositivo CPE. Tabelas de roteamento e encaminhamento virtual criadas no modelo de CPE são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma tabela de roteamento e encaminhamento virtual:

1. Crie uma tabela de roteamento e encaminhamento virtual de uma das seguintes formas:

   - Para criar uma tabela de roteamento e encaminhamento virtual em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRF**.
   - Para criar uma tabela de roteamento e encaminhamento virtual em um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **VRF**.

   Por padrão, é selecionada a guia **VRF**, que exibe a tabela de roteamento e encaminhamento virtual.

2. Clique em **+ VRF**.

3. Na janela aberta, no campo **Nome**, insira o nome da tabela de roteamento e encaminhamento virtual.

4. No campo **Tabela**, insira o ID da tabela de roteamento e encaminhamento virtual. Intervalo de valores: 100 a 199.

5. Para garantir isolamento de tráfego adicional para a tabela de roteamento e encaminhamento virtual, marque a caixa de seleção **Adicionar rota blackhole**. Como resultado, uma rota blackhole 0.0.0.0/0 é criada automaticamente ao salvar a tabela de roteamento e encaminhamento virtual na seção **Rotas estáticas**.

   Se essa rota estática já tiver sido criada, a caixa de seleção **Adicionar rota blackhole** é marcada ao criar uma tabela de roteamento e encaminhamento virtual. Desmarcar a caixa de seleção exclui a rota estática criada anteriormente.

   Esta caixa de seleção está desmarcada por padrão. Sem uma rota blackhole, o tráfego pode acabar em outras tabelas de roteamento e encaminhamento virtual.

6. Na lista suspensa **Interfaces**, selecione a interface de rede criada que deseja adicionar à tabela de roteamento e encaminhamento virtual. Não é possível adicionar a mesma interface de rede a múltiplas tabelas de roteamento e encaminhamento virtual.

   A instância de rede é adicionada e exibida na parte inferior da janela. É possível adicionar várias interfaces de rede ou excluir interfaces de rede. Para excluir uma interface de rede, clique em **Excluir** ao lado dela.

Caso tenha adicionado uma interface de rede com um nome no formato 'overlay.<número>' (por exemplo, 'overlay.100') à tabela de roteamento e encaminhamento virtual, marque as caixas de seleção **Ativa automaticamente** e **Forçar endereço IP, rota e gateway** ao criar ou editar a interface de rede.

7. Clique em **Criar**.

   A tabela de roteamento e encaminhamento virtual é criada e exibida na tabela. Uma interface de rede do sistema correspondente à tabela de roteamento e encaminhamento virtual criada é criada no dispositivo CPE. Se **Adicionar rota blackhole** foi selecionado, a rota blackhole 0.0.0.0/0 é criada automaticamente na seção **Rotas estáticas**.

8. Crie um registro na interface da Web do orquestrador para a interface de rede do sistema:

   a. Selecione a guia **Rede**.

      A tabela de interfaces de rede é exibida.

   b. Clique em **+ Interface de rede**.

   c. Na janela aberta, no campo **Alias**, insira o nome da tabela de roteamento e encaminhamento virtual especificada na etapa 3 destas instruções. O comprimento máximo do nome é de 15 caracteres.

   d. Se forem atribuídas zonas de firewall a interfaces de rede na tabela de roteamento e encaminhamento virtual e o firewall do dispositivo CPE não aceitar, por padrão, pacotes de tráfego encaminhados entre interfaces de rede e sub-redes, na lista suspensa **Zona**, selecione uma zona de firewall. A zona de firewall selecionada também deve ser atribuída a uma das interfaces de rede na tabela de roteamento e encaminhamento virtual.

   e. No campo **Nome da interface**, insira o nome da tabela de roteamento e encaminhamento virtual especificada na etapa 3 destas instruções. O comprimento máximo do nome é de 256 caracteres.

9. Clique em **Criar**.

   Um registro para a interface de rede do sistema é criado e exibido na tabela.

10. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Modificar a tabela de roteamento e encaminhamento virtual

É possível editar uma tabela de roteamento e encaminhamento virtual em um modelo de CPE ou em um dispositivo. Uma tabela de roteamento e encaminhamento virtual editada no modelo de CPE é automaticamente editada em todos os dispositivos CPE que usam o modelo. Não é possível editar uma tabela de roteamento e encaminhamento virtual herdada de um modelo de CPE em um dispositivo CPE.

Para editar uma tabela de roteamento e encaminhamento virtual:

1. Edite uma tabela de roteamento e encaminhamento virtual de uma das seguintes formas:

   - Para editar uma tabela de roteamento e encaminhamento virtual em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRF**.

   - Para editar uma tabela de roteamento e encaminhamento virtual em um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **VRF**.

Por padrão, é selecionada a guia **VRF**, que exibe a tabela de roteamento e encaminhamento virtual.

2. Clique em **Editar** ao lado da tabela de roteamento e encaminhamento virtual que deseja editar.

3. Na janela aberta, gerencie as configurações da tabela de roteamento e encaminhamento virtual.

4. Clique em **Salvar**.

   A tabela de roteamento e encaminhamento virtual é modificada e atualizada na tabela.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Excluir uma tabela de roteamento e encaminhamento virtual

É possível excluir uma tabela de roteamento e encaminhamento virtual em um modelo de CPE ou em um dispositivo CPE. Uma tabela de roteamento e encaminhamento virtual excluída do modelo de CPE é automaticamente excluída de todos os dispositivos CPE que usam o modelo. Não é possível excluir uma tabela de roteamento e encaminhamento virtual herdada de um modelo de CPE em um dispositivo CPE.

As tabelas de roteamento e encaminhamento virtual excluídas não podem ser restauradas.

Para excluir uma tabela de roteamento e encaminhamento virtual:

1. Exclua uma tabela de roteamento e encaminhamento virtual de uma das seguintes formas:

   - Para excluir uma tabela de roteamento e encaminhamento virtual em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **VRF**.

   - Para excluir uma tabela de roteamento e encaminhamento virtual em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE**, clique no dispositivo CPE e selecione a guia **VRF**.

   Por padrão, é selecionada a guia **VRF**, que exibe a tabela de roteamento e encaminhamento virtual.

2. Clique em **Excluir** ao lado da tabela de roteamento e encaminhamento virtual que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A tabela de roteamento e encaminhamento virtual é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Monitorar informações de pacotes de tráfego usando o protocolo NetFlow

O Kaspersky SD-WAN é compatível com as versões 1, 5 e 9 do NetFlow para o monitoramento de informações sobre pacotes de tráfego em um dispositivo CPE.

Os modelos de NetFlow são usados para a configuração centralizada do protocolo NetFlow em dispositivos CPE. Para evitar a configuração de cada dispositivo CPE individualmente, especifique as configurações básicas no modelo de NetFlow e aplique-o em dispositivos CPE ao adicioná-los ou registrá-los manualmente. Ao editar uma configuração em um modelo de NetFlow, a configuração é automaticamente modificada em todos os dispositivos CPE que estiverem usando o modelo. Ao editar uma configuração no dispositivo CPE, essa configuração se torna independente do modelo de NetFlow e, caso seja modificada no modelo de NetFlow, permanece inalterada no dispositivo CPE.

Ao especificar as configurações básicas de NetFlow, é possível especificar até quatro coletores NetFlow. Caso deseje que um dispositivo CPE envie informações sobre pacotes de tráfego para os coletores NetFlow, ative o protocolo NetFlow nas interfaces de rede. O protocolo NetFlow pode ser ativado ao criar ou editar a interface de rede.

Gerenciar modelos de NetFlow

Para visualizar a tabela de modelos de NetFlow, vá para a seção **SD-WAN → Modelos NetFlow**. Por padrão, um **modelo de NetFlow padrão** é criado no portal do administrador e se torna a base para todos os outros modelos de NetFlow criados. As informações sobre modelos de NetFlow são exibidas nas seguintes colunas da tabela:

- **ID** é o ID do modelo de NetFlow.
- **Nome** é o nome do modelo de NetFlow.
- **Utilização** especifica se os dispositivos CPE usam o modelo de NetFlow:
  - **Sim**.
  - **Não**.
- **Atualizado** é a data e hora em que as configurações do modelo de CPE foram modificadas pela última vez.
- **Usuário** é o nome do usuário que criou o modelo de NetFlow.
- **Proprietário** é o locatário ao qual o modelo de NetFlow pertence.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

É possível selecionar um modelo de NetFlow atribuído para ser pré-selecionado ao adicionar ou registrar manualmente um dispositivo CPE. Para locatários, crie e selecione manualmente um modelo de NetFlow atribuído no portal de autoatendimento.

Criar um modelo de NetFlow

Para criar um modelo de NetFlow:

1. No menu, acesse a seção **SD-WAN → Modelos NetFlow**.

   Uma tabela de modelos de NetFlow é exibida.

2. Na parte superior da página, clique em **+ Modelo NetFlow**.

3. Na janela aberta, insira o nome do modelo de NetFlow.

4. Clique em **Criar**.

   O modelo de NetFlow é criado e exibido na tabela.

É necessário configurar o modelo de NetFlow criado. Para obter detalhes sobre as configurações do modelo de NetFlow, consulte as instruções sobre como definir as configurações básicas do NetFlow.

Selecionar um modelo de NetFlow atribuído

É possível selecionar um modelo de NetFlow atribuído para ser pré-selecionado ao adicionar ou registrar manualmente um dispositivo CPE. Para locatários, crie e selecione manualmente um modelo de NetFlow atribuído no portal de autoatendimento.

Para selecionar um modelo de NetFlow atribuído:

1. No menu, acesse a seção **SD-WAN → Modelos NetFlow**.

   Uma tabela de modelos de NetFlow é exibida.

2. Clique no modelo de NetFlow que deseja tornar o modelo atribuído.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Definir como designado**.

   O modelo de NetFlow se torna o modelo atribuído.

Importar um modelo de NetFlow

É possível exportar um modelo de NetFlow e depois importá-lo para outro modelo de NetFlow. As configurações do modelo de NetFlow são especificadas de acordo com as configurações do modelo de NetFlow importado. Durante a importação, selecione as configurações que deseja deixar inalteradas. O modelo de NetFlow para o qual você está importando outro modelo de NetFlow permanece aplicado aos dispositivos CPE, mas as configurações desses dispositivos CPE não são modificadas.

Para importar um modelo de NetFlow:

1. No menu, vá para a seção **SD-WAN → Modelos NetFlow**.

   Uma tabela de modelos de NetFlow é exibida.

2. Clique no modelo de NetFlow que deseja exportar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Exportar**.

   Um arquivo comprimido no formato TAR.GZ é salvo no dispositivo local. O arquivo não contém informações sobre dispositivos CPE que usam o modelo de NetFlow.

4. Clique no modelo de NetFlow para o qual deseja importar outro modelo de NetFlow.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃.

5. Na parte superior da área de configurações, em **Ações**, clique em **Importar**.

6. Na janela aberta, desmarque as caixas de seleção ao lado das configurações do modelo de NetFlow que deseja manter inalteradas após a importação.

7. No campo **Arquivo**, especifique o caminho para o arquivo TAR.GZ.

8. Clique em **Importar**.

As configurações do modelo de NetFlow são alteradas de acordo com as configurações do modelo de NetFlow importado.

Clonar um modelo de NetFlow

É possível clonar um modelo de NetFlow para criar um modelo idêntico com um nome diferente.

Para clonar um modelo de NetFlow:

1. No menu, vá para a seção **SD-WAN → Modelos NetFlow**.

   Uma tabela de modelos de NetFlow é exibida.

2. Clique no modelo de NetFlow que deseja clonar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Clonar**.

4. Na janela aberta, insira o nome do novo modelo de NetFlow.

5. Clique em **Clonar**.

Um clone do modelo de NetFlow com o novo nome é criado e exibido na tabela.

Visualizar o uso de um modelo de NetFlow

Se necessário, é possível verificar quais dispositivos CPE estão usando o modelo de NetFlow. Por exemplo, se um modelo de NetFlow estiver em uso, ele não pode ser excluído.

Para ver se um modelo de NetFlow está sendo usado:

1. No menu, acesse a seção **SD-WAN → Modelos NetFlow**.

   Uma tabela de modelos de NetFlow é exibida.

2. Clique no modelo de NetFlow cujas informações de uso deseja visualizar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Mostrar utilização**.

Isso abre uma janela com uma tabela de dispositivos CPE que estão usando o modelo de NetFlow.

Excluir um modelo de NetFlow

Não é possível excluir um modelo de NetFlow se ele estiver sendo usado por pelo menos um dispositivo CPE. Para excluir um modelo de NetFlow que está sendo usado por dispositivos CPE, primeiro altere o modelo de NetFlow dos dispositivos CPE. É possível verificar quais dispositivos CPE estão usando o modelo de NetFlow.

Os modelos de NetFlow excluídos não podem ser restaurados.

Para excluir um modelo de NetFlow:

1. No menu, acesse a seção **SD-WAN → Modelos NetFlow**.

   Uma tabela de modelos de NetFlow é exibida.

2. Clique no modelo de NetFlow que deseja excluir.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

O modelo de NetFlow é excluído e não é mais exibido na tabela.

Configurações básicas de NetFlow

É possível especificar configurações básicas de NetFlow em um modelo de NetFlow ou dispositivo CPE. As configurações básicas de NetFlow especificadas no modelo de NetFlow são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para modificar as configurações básicas de NetFlow:

1. Especifique as configurações básicas de NetFlow de uma das seguintes formas:

   - Para editar as configurações básicas de NetFlow em um modelo de NetFlow, vá para a seção **SD-WAN** → **Modelos NetFlow** do menu e clique no modelo de NetFlow.

   - Para editar as configurações básicas de NetFlow em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **NetFlow** e marque a caixa de seleção **Substituir**.

   As configurações básicas de NetFlow são exibidas.

2. Na lista suspensa **NetFlow**, selecione **Ativado**. O valor padrão é **Desativado**.

3. Especifique o coletor NetFlow:

   a. Em **Coletores**, clique em **+ Adicionar**.

   b. Em **Host**, insira o endereço IPv4 do coletor NetFlow.

   c. Em **Porta**, insira o número da porta do coletor NetFlow. Intervalo de valores: 1 a 65.535.

   O coletor NetFlow é especificado e exibido na seção **Coletores**. É possível especificar até quatro coletores NetFlow ou excluir um coletor NetFlow. Para excluir um coletor do NetFlow, clique no ícone de exclusão ✕ ao lado dele.

4. Na lista suspensa **Exportar versão**, selecione a versão do protocolo NetFlow:

   - **1**

   - **5**

   - **9**. Essa é a configuração padrão.

5. Na lista suspensa **Nível de rastreamento**, selecione as informações de pacotes de tráfego que o dispositivo CPE rastreia:

   - **ETHER** para rastrear as seguintes informações:

     - Endereços IP e portas de origem e destino

     - Endereços MAC de origem e destino

     - Tag da VLAN externa

     - Protocolo sendo usado

   - **FULL** para rastrear os endereços IP e portas de origem e destino, bem como o protocolo sendo usado. Essa é a configuração padrão.

- **VLAN** para rastrear as seguintes informações:
  - Endereços IP e portas de origem e destino
  - Tag da VLAN externa
  - Protocolo sendo usado
- **PROTO** para rastrear os endereços IP de origem e destino e o protocolo sendo usado.
- **IP** para rastrear os endereços IP de origem e destino.

6. No campo **Máximo de fluxos**, insira o número máximo de fluxos de tráfego que o dispositivo CPE pode rastrear simultaneamente. Intervalo de valores: 1 a 65.535. O valor padrão é `8192`.

   Quanto maior o valor, maior a carga na CPU no dispositivo CPE.

7. No campo **Taxa de amostragem**, especifique a frequência com que o dispositivo CPE rastreia as informações do pacote de tráfego. Por exemplo, ao inserir `10`, o dispositivo CPE rastreará as informações de cada décimo pacote de tráfego. Intervalo de valores: 1 a 8192. O valor padrão é `1024`.

   Quanto menor o valor, mais precisas as informações e maior a carga na CPU no dispositivo CPE.

8. No campo **Tempo limite máximo (s)**, insira o tempo máximo, em segundos, durante o qual o dispositivo CPE pode rastrear informações de fluxo de tráfego. Para desativar esse recurso, insira `0`. Intervalo de valores: 1 a 9999. O valor padrão é `60`.

9. No campo **Limite de saltos**, insira o número máximo de saltos para os coletores NetFlow. Intervalo de valores: 1 a 255. O valor padrão é `64`.

10. Para que o dispositivo CPE rastreie o tráfego IPv6, na lista suspensa **Rastrear IPv6**, selecione **Ativado**. O valor padrão é **Desativado**.

11. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de NetFlow ou dispositivo CPE.

Caso deseje que um dispositivo CPE envie informações sobre pacotes de tráfego para os coletores NetFlow, ative o protocolo NetFlow nas interfaces de rede. O protocolo NetFlow pode ser ativado ao criar ou editar a interface de rede.

Alterar o modelo de NetFlow de um dispositivo CPE

Para alterar o modelo de NetFlow de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE para o qual deseja alterar o modelo de NetFlow.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na lista suspensa **Modelo NetFlow**, selecione um modelo de NetFlow criado.

4. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

Diagnosticar um dispositivo CPE

É possível solicitar informações de diagnóstico de um dispositivo CPE, como o uso do protocolo BGP, OSPF e PIM. As informações de diagnóstico retornadas em resposta à solicitação são exibidas na interface da Web do orquestrador e, se necessário, podem ser baixadas em um arquivo TXT.

O Kaspersky SD-WAN também é compatível com os seguintes utilitários para diagnóstico de dispositivos CPE:

- O Ping é um utilitário para testar o link entre um dispositivo CPE e um endereço IPv4 especificado.
- O Traceroute é um utilitário para determinar a rota entre um dispositivo CPE e um endereço IPv4 especificado.
- O Tcpdump é um utilitário para capturar o tráfego em um dispositivo CPE. Capturar significa que é feita uma cópia do tráfego e o tráfego original é retransmitido para seu destino.
- O Iperf é um utilitário para diagnosticar o desempenho da rede. É possível usar o dispositivo CPE como um servidor iperf ou um cliente iperf.
- O Sweep é um utilitário para executar as seguintes ações em um dispositivo CPE:
  - Limpar o cache ARP
  - Reiniciar o processo FRR (Free Range Routing)
  - Limpar a tabela de sessão NAT
  - Reiniciar modems
- O OpenFlow dump é um utilitário para solicitar fluxos de despejo e grupos de despejo gerados pelo switch virtual de um dispositivo CPE.

Os utilitários tcpdump, iperf e OpenFlow dump geram relatórios que podem ser baixados ou excluídos.

A execução de um utilitário é uma tarefa que o dispositivo CPE recebe do orquestrador; a tarefa obedece ao período configurado para o dispositivo CPE enviar solicitações de API REST ao orquestrador. Caso deseje que os utilitários sejam executados antes, ative o modo interativo no dispositivo CPE.

No *modo interativo*, o dispositivo CPE usa um intervalo de tempo mais curto para enviar solicitações de API REST ao orquestrador. O modo interativo termina automaticamente quando a duração especificada tiver passado. É possível especificar as seguintes configurações do modo interativo ao configurar a conexão de um dispositivo CPE ao orquestrador e controlador:

- O período de espera até que o dispositivo CPE envie outra solicitação de API REST ao orquestrador no modo interativo
- O tempo após o qual o modo interativo é automaticamente desativado

Solicitar informações de diagnóstico

Para solicitar informações de diagnóstico:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE sobre o qual deseja solicitar informações de diagnóstico.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Informações de diagnóstico**.

   Os parâmetros de solicitação de informações de diagnóstico são exibidos.

4. Clique em **Solicitar informações de diagnóstico**.

   Aguarde até que as informações de diagnóstico sejam recebidas do dispositivo CPE.

5. Na lista suspensa **Nome**, selecione que tipo de informações de diagnóstico deseja exibir:

   - **disk usage** para informações sobre o uso do disco do dispositivo CPE. Essa é a configuração padrão.
   - **ip addresses** para informações sobre endereços IP atribuídos a portas físicas ou interfaces virtuais do sistema operacional do dispositivo CPE.
   - **vrf data** para informações sobre tabelas de roteamento e encaminhamento virtual.
   - **ip neighbors** para informações sobre os vizinhos IP do dispositivo CPE, obtidas da tabela ARP ou usando o Protocolo de descoberta de vizinhos.
   - **ip routes** para informações sobre rotas IPv4 e IPv6.
   - **ip rules** para informações sobre regras de roteamento.
   - **iptables** para informações sobre o iptables.
   - **cpe log** para o log local do dispositivo CPE.
   - **ovs-ofctl show** para informações sobre o switch virtual.
   - **ovs-vsctl show** para informações sobre o link entre o switch virtual e os controladores.

- **ovs-vsctl list controller** para informações sobre os controladores especificados para o switch virtual.
- **show ip ospf** para informações sobre o processo de roteamento OSPF.
- **show ip ospf interface** para informações sobre interfaces OSPF.
- **show ip ospf neighbor** para informações sobre os vizinhos OSPF.
- **show ip ospf database** para o banco de dados OSPF.
- **bgp show ip route** para informações sobre rotas BGP.
- **show ip bgp** para informações sobre o processo de roteamento BGP.
- **show ip bgp summary** para informações rápidas sobre o processo de roteamento BGP.
- **top process** para informações sobre processos do Linux.
- **uptime** para informações sobre o tempo de atividade do dispositivo CPE.
- **time sync** para informações sobre a sincronização de tempo no dispositivo CPE usando um servidor NTP.
- **netstat** para informações sobre links de rede que o dispositivo CPE estabeleceu.
- **sdwan interfaces** para informações sobre interfaces SD-WAN.
- **modems** para informações sobre modems.

  As informações recebidas do dispositivo também são exibidas na seção **Modems** da área de configurações do dispositivo CPE (**SD-WAN** → **CPE**).
- **show bfd peers** para informações sobre pares BFD.
- **netflow dump-flows** para informações sobre fluxos NetFlow.
- **netflow statistics** para informações sobre o uso do protocolo NetFlow.
- **show bfd peers brief** para informações breves sobre pares BFD.
- **show ip pim bsr** para informações sobre o roteador bootstrap atual (BSR).
- **show ip pim bsrp-info** para informações sobre o mapeamento group-to-rp recebido do roteador bootstrap.
- **show ip pim interface** para informações sobre as interfaces PIM. É possível configurar o protocolo PIM ao criar ou editar uma interface multicast.
- **show ip pim interface traffic** para informações sobre o tráfego PIM.
- **show ip pim join** para informações sobre grupos multicast aos quais o dispositivo CPE está conectado.
- **show ip pim neighbor** para informações sobre vizinhos PIM.
- **show ip pim nexthop** para informações sobre os próximos saltos de grupos multicast.

- **show ip pim rp-info** para informações sobre pontos de encontro. É possível especificar pontos de encontro ao especificar configurações básicas de PIM.
- **show ip pim secondary** para informações sobre o roteador PIM de backup.
- **show ip pim state** para informações sobre o estado do protocolo PIM.
- **show ip pim statistics** para informações sobre o uso do protocolo PIM.
- **show ip pim upstream** para informações sobre fontes PIM.
- **show ip igmp groups** para informações sobre grupos IGMP.
- **show ip igmp interface** para informações sobre interfaces IGMP. É possível configurar o IGMP ao criar ou editar uma interface multicast.
- **show ip igmp interface detail** para informações detalhadas sobre as interfaces IGMP.
- **show ip igmp sources** para informações sobre fontes IGMP.
- **igmp statistics** para informações sobre o uso do IGMP.
- **show ip multicast** para informações sobre o processo de roteamento multicast.
- **show ip mroute** para informações sobre rotas multicast.
- **show ip mroute summary** para informações rápidas sobre rotas multicast.
- **vswitchd log** para o log do processo ovs-vswitchd.
- **firewall config** para informações sobre o firewall.
- **sw version** para a versão do firmware do dispositivo CPE.
- **vrrp stats** para informações rápidas sobre o uso do VRRP.
- **vrrp data** para informações sobre o uso do VRRP.

6. Para filtrar as informações de diagnóstico exibidas:

   a. No campo **Encontrar linha por padrão**, insira as palavras que devem estar nas linhas de informações de diagnóstico a serem exibidas. Comprimento máximo: 64 caracteres. Para exibir apenas linhas que não contenham as palavras inseridas, marque a caixa de seleção **Mostrar tudo menos encontrados**. Esta caixa de seleção está desmarcada por padrão.

   b. No campo **Mostrar linhas antes e depois**, insira o número de linhas em branco que deseja exibir antes e depois de cada linha de informações de diagnóstico.

7. Para baixar o arquivo com as informações de diagnóstico, clique em **Baixar**.

   Um arquivo TXT é salvo em seu dispositivo local.

Usar o modo de depuração para protocolos de roteamento dinâmico em dispositivos CPE

É possível usar o modo de depuração para a solução detalhada de problemas dos protocolos BGP e OSPF em dispositivos CPE. Ao ativar o modo de depuração em um dispositivo CPE, o nível do registro para os logs do processo FRR é definido como Depuração e os comandos **debug** <...> relevantes do pacote FRR são executados no dispositivo.

Ativar o modo de depuração no CPE pode aumentar significativamente a carga da CPU. Recomendamos fazer isso fora do horário comercial para evitar problemas de desempenho. Se o dispositivo CPE ficar indisponível após a ativação do modo de depuração, desative o modo de depuração no orquestrador e reinicie o dispositivo CPE.

Para ativar o modo de depuração:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja ativar o modo de depuração.

3. A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

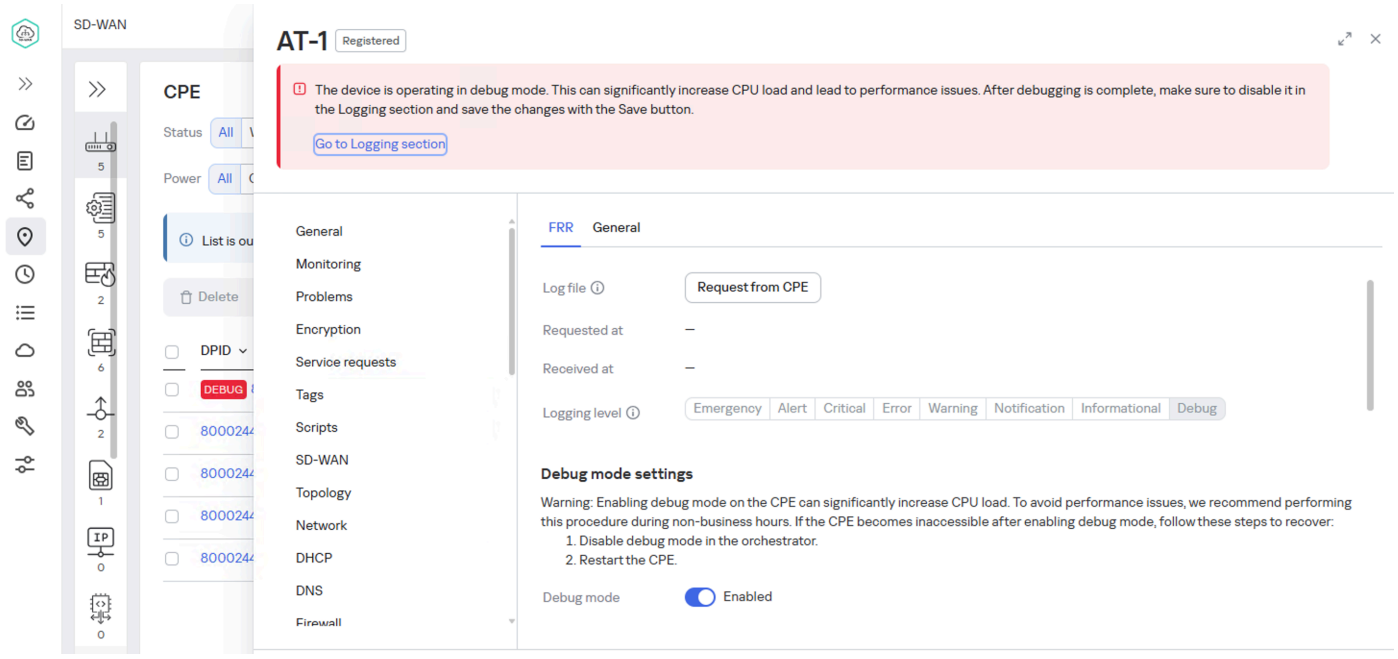
4. No menu à esquerda, selecione a seção **Logs** e, em seguida, a guia **FRR**.

5. Ative o botão **Modo de depuração**.

6. Nas guias **BGP** e **OSPF** exibidas, especifique as opções para os comandos de depuração FRR conforme necessário. Para ativar o modo de depuração, é necessário especificar pelo menos uma opção em qualquer uma das guias.

7. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do dispositivo CPE ou agende um salvamento posterior clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

O dispositivo CPE em que o modo de depuração está ativado é exibido na tabela na seção **SD-WAN → CPE**, com o ícone DEBUG ao lado do DPID.



O dispositivo CPE está no modo de depuração

Para baixar o arquivo de registro de depuração, solicite-o ao dispositivo clicando no botão **Solicitação do CPE** (ou **Atualização do CPE** se o arquivo já tiver sido solicitado anteriormente) e, após aguardar o arquivo ser carregado no orquestrador, clique no link de download. O conteúdo do arquivo é substituído a cada nova solicitação. Observe que o espaço de armazenamento limitado é alocado para o arquivo e, quando o limite é atingido, novos registros não são adicionados ao arquivo.

Especificar servidores NTP em dispositivos CPE

É necessário especificar um servidor NTP interno ou externo ou um pool de servidores para dispositivos CPE, de forma a assegurar que a hora exata seja exibida nos dispositivos. É possível usar um dispositivo CPE como servidor NTP para exibir a hora exata em dispositivos de rede conectados a ele.

É possível especificar o servidor NTP em um modelo de CPE ou no dispositivo CPE. Servidores NTP especificados no modelo de CPE são especificados automaticamente em todos os dispositivos CPE que usam o modelo.

Para especificar o servidor NTP em dispositivos CPE:

1. Especifique o servidor NTP de uma das seguintes formas:

   - Para especificar o servidor NTP em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **NTP**.

   - Para especificar um servidor NTP em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **NTP** e marque a caixa de seleção **Substituir**.

   As configurações de conexão do servidor NTP são exibidas.

2. Se não desejar especificar o servidor NTP para o dispositivo CPE, desmarque a caixa de seleção **Conectar ao servidor NTP**. Esta caixa de seleção é selecionada por padrão.

3. Para usar o dispositivo CPE como servidor NTP, marque a caixa de seleção **Usar CPE como servidor NTP**. Esta caixa de seleção está desmarcada por padrão.

4. Especifique um servidor NTP ou um pool de servidores:

   a. Em **Servidores NTP**, clique em **+ Adicionar**.

   b. No campo exibido, insira o endereço IP ou FQDN do servidor NTP ou do pool de servidores. Os seguintes formatos de endereço IP e FQDN são compatíveis:

      - Para especificar um servidor NTP, insira o endereço IP ou FQDN no formato `server <endereço IP ou FQDN>`; por exemplo, `server 0.pool.ntp.org`.

      - Para especificar um pool de servidores NTP, insira o endereço IP ou FQDN no formato `pool <endereço IP ou FQDN>`; por exemplo, `pool pool.ntp.org`.

   O servidor NTP é especificado e exibido na seção **Servidores NTP**. É possível especificar vários servidores NTP ou excluir servidores NTP. Para excluir um servidor NTP, clique no ícone de exclusão ✕ ao lado dele.

5. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Solicite informações de diagnóstico para ver as configurações de sincronização de tempo em um dispositivo CPE.

Ativar o modo interativo

É possível especificar as seguintes configurações do modo interativo ao configurar a conexão de um dispositivo CPE ao orquestrador e controlador:

- O período de espera até que o dispositivo CPE envie outra solicitação de API REST ao orquestrador no modo interativo

- O tempo após o qual o modo interativo é automaticamente desativado

Para ativar o modo interativo:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja ativar o modo interativo.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na parte superior da área de configurações, clique em **Modo interativo**.

O modo interativo é ativado no dispositivo CPE.

Executar o utilitário ping

Para executar o utilitário ping:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja executar o utilitário ping.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários**.

   Por padrão, é selecionada a guia **Ping**, que exibe as configurações do utilitário ping.

4. No campo **Endereço IP de destino**, insira o endereço IPv4 para o qual o dispositivo CPE envia solicitações ICMP.

5. Caso deseje que o dispositivo CPE envie solicitações ICMP de uma interface de rede criada, na lista suspensa **Interface de rede de origem**, selecione a interface de rede.

6. No campo **Contagem**, insira o número de solicitações ICMP que o dispositivo CPE envia. Intervalo de valores: 1 a 1.000.000. O valor padrão é `5`.

7. No campo **Tempo limite (s)**, insira o tempo em segundos após o qual o dispositivo CPE deve receber uma resposta ICMP para considerar a solicitação bem-sucedida. Intervalo de valores: 1 a 3600. O valor padrão é `2`.

8. No campo **Tamanho**, insira o tamanho da solicitação ICMP em bytes. Intervalo de valores: 1 a 65.535. O valor padrão é `56`.

9. No campo **TTL**, insira o número máximo de saltos para solicitações ICMP. Intervalo de valores: 1 a 255. O valor padrão é `255`.

10. No campo **Intervalo**, insira o intervalo em segundos para o dispositivo CPE usar ao enviar solicitações ICMP para o endereço IPv4 especificado. Intervalo de valores: 1 a 300. O valor padrão é `1`.

11. Clique em **Executar**.

O utilitário ping é executado no dispositivo CPE e um relatório contendo o resultado do utilitário ping é exibido na parte inferior da área de configurações.

Executar o utilitário traceroute

Para executar o utilitário traceroute:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja executar o utilitário traceroute.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários → Traceroute (ferramenta de rastrear dados)**.

   As configurações do utilitário traceroute são exibidas.

4. No campo **Endereço IP de destino**, insira o endereço IPv4 para o qual o dispositivo CPE envia a série de solicitações ICMP.

5. Caso deseje que o dispositivo CPE envie a série de solicitações ICMP de uma interface de rede criada, na lista suspensa **Interface de origem**, selecione a interface de rede.

6. Caso deseje que o dispositivo CPE use o servidor DNS para resolver endereços IP para nomes de domínio ao criar o relatório com o resultado do utilitário traceroute, marque a caixa de seleção **Resolver nomes DNS**. É possível especificar um servidor DNS ao criar ou editar uma interface de rede. Os endereços IP que não puderem ser resolvidos para nomes de domínio também são exibidos no relatório. Esta caixa de seleção está desmarcada por padrão.

7. No campo **Tempo limite de sondagem (s)**, insira o tempo em segundos após o qual o dispositivo CPE deve receber uma série de respostas ICMP para considerar a série de solicitações ICMP bem-sucedida. Intervalo de valores: 1 a 30. O valor padrão é `3`.

8. No campo **Número máximo de saltos**, insira o número máximo de saltos para a série de solicitações ICMP. Intervalo de valores: 1 a 60. O valor padrão é `10`.

9. Clique em **Executar**.

O utilitário traceroute é executado no dispositivo CPE e um relatório contendo o resultado do utilitário traceroute é exibido na parte inferior da área de configurações.

Executar o utilitário tcpdump

O utilitário tcpdump gera um relatório com o tráfego capturado. Ao executar o utilitário tcpdump novamente, o relatório é substituído. É possível baixar o relatório caso deseje mantê-lo.

O utilitário tcpdump coloca carga adicional na CPU do dispositivo CPE.

Para executar o utilitário tcpdump:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja executar o utilitário tcpdump.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários → Tcpdump**.

   As configurações do utilitário tcpdump são exibidas.

4. Na lista suspensa **Capturar interface de rede**, selecione a interface de rede criada na qual deseja capturar o tráfego.

5. Na lista suspensa **Direção**, selecione a direção do tráfego que deseja capturar:

   - **Entrada** para capturar o tráfego de entrada.
   - **Saída** para capturar o tráfego de saída.
   - **Entrada/Saída** para capturar o tráfego de entrada e de saída. Essa é a configuração padrão.

6. Caso deseje que o dispositivo CPE use o servidor DNS para resolver endereços IP para nomes de domínio ao criar o relatório com o tráfego capturado, marque a caixa de seleção **Resolver nomes DNS**. É possível especificar um servidor DNS ao criar ou editar uma interface de rede. Os endereços IP que não puderem ser resolvidos para nomes de domínio também são refletidos no relatório. Esta caixa de seleção está desmarcada por padrão.

7. Para usar um filtro para capturar o tráfego, no campo **Filtrar tcpdump**, insira a sintaxe do filtro. O comprimento máximo do filtro é de 1024 caracteres. Por exemplo, os seguintes filtros podem ser usados:

   - `icmp` para capturar apenas pacotes de tráfego ICMP.
   - `host 1.2.3.4 e (port 80 or 443)` para capturar apenas pacotes de tráfego com endereço IPv4 1.2.3.4 e porta TCP de origem ou destino 80 ou 443.
   - `tcp[13] & 2 != 0` para capturar apenas pacotes de tráfego TCP SYN.

   Informações detalhadas sobre filtros de tráfego podem ser obtidas na documentação oficial do tcpdump.

8. No campo **Tempo máximo de captura (s)**, insira o tempo em segundos após o qual a captura de tráfego é interrompida. Intervalo de valores: 10 a 600. O valor padrão é `30`.

9. No campo **Número máximo de pacotes capturados**, insira o número de pacotes de tráfego que deseja coletar antes que a captura de tráfego seja interrompida. Intervalo de valores: 1 a 10.000. O valor padrão é `1000`.

   A captura de tráfego é interrompida quando o tempo especificado no campo **Tempo máximo de captura (s)** passa ou quando o número de pacotes de tráfego especificado no campo **Número máximo de pacotes capturados** é capturado.

10. Clique em **Executar**.

O utilitário tcpdump é executado no dispositivo CPE e um relatório com o tráfego capturado é gerado.

Executar o utilitário iperf

O utilitário iperf gera um relatório com os resultados do diagnóstico de desempenho da rede. Ao executar o utilitário iperf novamente, o relatório é substituído. É possível baixar o relatório caso deseje mantê-lo.

Para executar o utilitário iperf:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja executar o utilitário iperf.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários → Iperf**.

   As configurações do utilitário iperf são exibidas.

4. Especifique o modo em que deseja usar o utilitário iperf no dispositivo CPE selecionando uma das seguintes opções:

   - **Servidor** para usar o dispositivo CPE como servidor iperf.
   - **Cliente** para usar o dispositivo CPE como cliente iperf.

5. Caso tenha escolhido a opção **Servidor**, configure o servidor iperf:

   a. No campo **Porta**, insira o número da porta TCP ou UDP do servidor iperf. Intervalo de valores: 1001 a 65.535. O valor padrão é `7777`.

   b. No campo **Intervalo de relatório (s)**, insira o intervalo em segundos para gravar linhas no relatório. Intervalo de valores: 0 a 60. O valor padrão é `3`.

   c. Caso não queira criar um relatório com os resultados do diagnóstico de desempenho da rede, marque a caixa de seleção **Nenhum relatório**. Esta caixa de seleção está desmarcada por padrão.

d. Em **Formato de relatório**, selecione o formato dos resultados do diagnóstico de desempenho da rede no relatório:

- **Kbit/s**. Essa é a configuração padrão.
- **Mbit/s**.
- **Kbyte/s**.
- **Mbyte/s**.

e. No campo **Executar por (s)**, insira o tempo em segundos durante o qual o servidor iperf deve ser executado. Intervalo de valores: 60 a 3600. O valor padrão é `300`.

6. Caso tenha escolhido a opção **Cliente**, configure o cliente iperf:

a. No campo **IP do servidor**, insira o endereço IPv4 do servidor iperf com o qual o cliente iperf estabelece conexão.

b. No campo **Porta**, insira o número da porta TCP ou UDP do servidor iperf com o qual o cliente iperf estabelece conexão. Intervalo de valores: 1001 a 65.535. O valor padrão é `7777`.

c. No campo **Intervalo de relatório (s)**, insira o intervalo em segundos para gravar linhas no relatório de diagnóstico de desempenho. Intervalo de valores: 0 a 60. O valor padrão é `3`.

d. Caso não queira criar um relatório com os resultados do diagnóstico de desempenho da rede, marque a caixa de seleção **Nenhum relatório**. Esta caixa de seleção está desmarcada por padrão.

e. Em **Formato de relatório**, selecione o formato dos resultados do diagnóstico de desempenho da rede no relatório:

- **Kbit/s**. Essa é a configuração padrão.
- **Mbit/s**.
- **Kbyte/s**.
- **Mbyte/s**.

f. No campo **Executar cliente por (s)**, insira o tempo em segundos durante o qual o cliente iperf deve ser executado. Intervalo de valores: 60 a 3600. O valor padrão é `60`.

g. Especifique o tipo de porta do servidor iperf selecionando uma das seguintes opções:

- **TCP**. Essa é a configuração padrão.
- **UDP**.

h. No campo **Taxa de bits do cliente**, insira a taxa de bits do cliente iperf em um dos seguintes formatos:

- `<taxa de bits em kbps>k` ou `<taxa de bits em kbps>K`

  Por exemplo, ao inserir `10000K`, a taxa de bits será de 10.000 kbps.

- `<taxa de bits em Mbps>m` ou `<taxa de bits em Mbps>M`

  Por exemplo, ao inserir `10M`, a taxa de bits será de 10 Mbps.

i. Na lista suspensa **Direção de teste**, selecione a direção do tráfego que deseja usar para medir o desempenho da rede:

- **Cliente-servidor** para usar o tráfego que o cliente iperf envia para o servidor iperf. Essa é a configuração padrão.
- **Servidor-cliente** para usar o tráfego que o servidor iperf envia para o cliente iperf.
- **Bidirecional** para usar o tráfego que o cliente iperf envia ao servidor iperf, bem como o tráfego que o servidor iperf envia ao cliente iperf.

j. Se necessário, no campo **Janelas TCP (bytes)**, insira o tamanho da janela TCP em bytes. Se esse campo for deixado em branco, o tamanho da janela TCP será determinado automaticamente.

k. Se necessário, no campo **MSS de TCP (bytes)**, insira o tamanho máximo do segmento TCP em bytes.

7. Clique em **Executar**.

O utilitário iperf é executado no dispositivo CPE e um relatório com os resultados do diagnóstico de rede é gerado.

Para gerenciar relatórios, clique em **Ir para arquivos**.

Executar o utilitário sweep

O utilitário sweep pode ser usado para limpar o cache ARP, reiniciar o processo de Free Range Routing (FRR), limpar a tabela de sessões NAT ou reiniciar um modem em um dispositivo CPE.

Reiniciar o processo de FRR e limpar a tabela de sessões NAT pode fazer com que a transmissão do tráfego pare por alguns segundos.

Para executar o utilitário sweep:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja executar o utilitário sweep.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários → Varredura**.

   As configurações do utilitário sweep são exibidas.

4. Para limpar o cache ARP:

   a. Em **Limpar cache ARP**, selecione a interface de rede criada na qual deseja limpar o cache ARP. Para limpar o cache ARP em todas as interfaces de rede, selecione **Todos**.

   b. Clique em **Executar**.

O cache ARP é limpo no dispositivo CPE.

5. Para reiniciar o processo de FRR, em **Processo FRR**, clique em **Executar**.

   O processo de FRR é reiniciado no dispositivo CPE.

6. Para limpar a tabela de sessões NAT, em **Tabela de sessões de NAT**, clique em **Executar**. É possível configurar o NAT em um dispositivo CPE usando um firewall.

   A tabela de sessões NAT é limpa no dispositivo CPE.

7. Para reiniciar um modem, em **Modem**, selecione o modem na lista **Redefinir modem** e clique no botão **Executar**.

   O modem é reiniciado no dispositivo CPE.

Executar o utilitário OpenFlow dump

O utilitário OpenFlow dump gera um relatório com os fluxos de despejo e grupos de despejo solicitados. Ao executar o utilitário OpenFlow dump novamente, o relatório é substituído. É possível baixar o relatório caso deseje mantê-lo.

Para executar o utilitário OpenFlow dump:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja executar o utilitário OpenFlow dump.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários → Despejo OpenFlow**.

   As opções do utilitário OpenFlow dump são exibidas.

4. Clique em **Executar**.

   O utilitário OpenFlow dump é executado no dispositivo CPE e um relatório é gerado com os fluxos de despejo e grupos de despejo solicitados.

Para gerenciar relatórios, clique em **Ir para arquivos**.

Redefinir sessões de BGP/OSPF

É possível emitir comandos de redefinição/limpeza para sessões de BGP e OSPF em um dispositivo CPE. Para executar esses comandos, crie uma solicitação de limpeza que consista em um ou mais comandos de `limpeza`.

Para criar e executar uma solicitação de limpeza:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual deseja executar os comandos de limpeza.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários** → **Limpar BGP/OSPF**.

   As opções para a criação de comandos de limpeza são exibidas.

4. Clique em **Criar**.

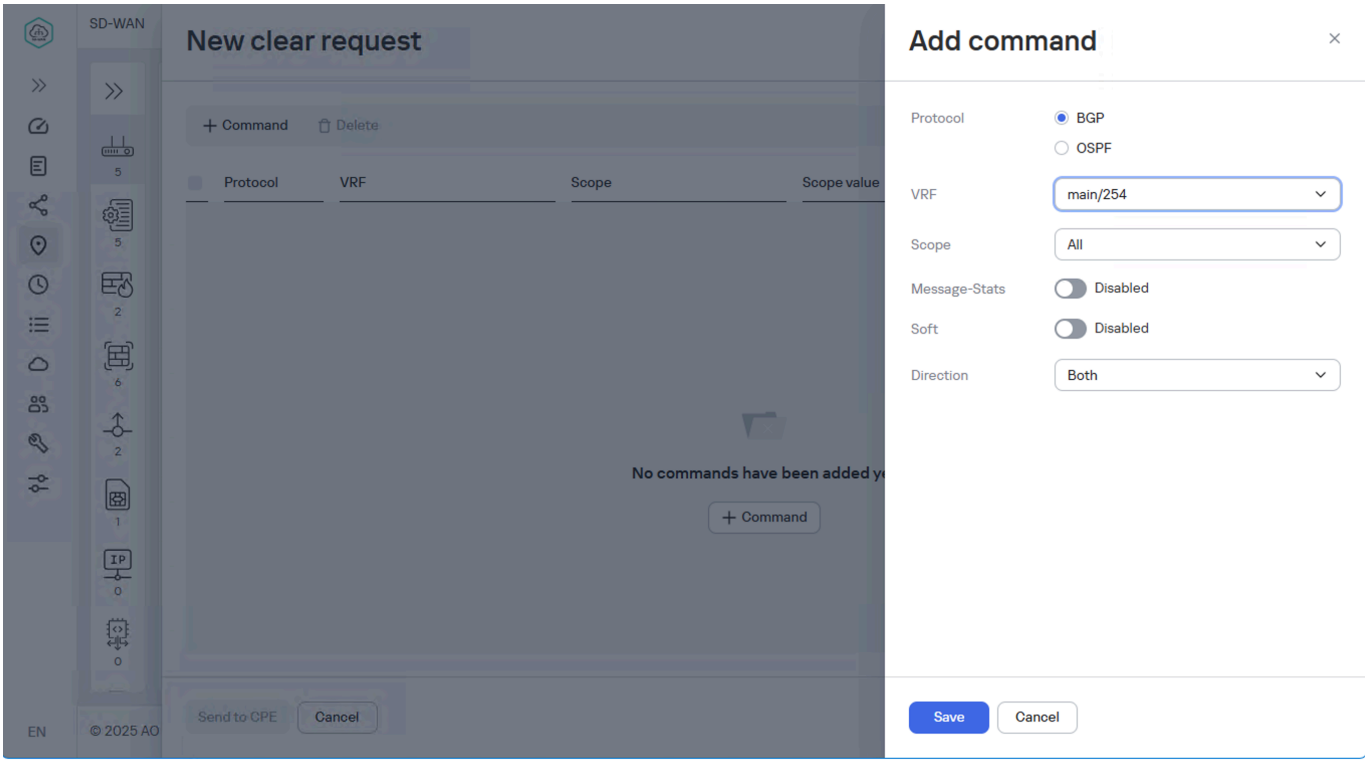
   Isso abre a área de criação de solicitação de limpeza com uma tabela que lista os comandos de limpeza sendo criados.

5. Clique no botão **Criar** para adicionar um ou mais comandos:

   a. Na área de criação de comandos, no campo **Protocolo**, selecione um protocolo (**BGP** ou **OSPF**).

   b. Especifique as opções do comando de limpeza para o protocolo selecionado.

   c. Clique em **Salvar** para salvar as opções de comando.

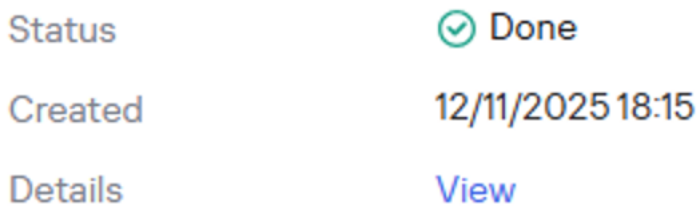


Adicionar um comando de limpeza

   O comando é adicionado à tabela. Se necessário, selecione um comando na tabela e exclua-o clicando no botão **Excluir**.

6. Clicar no botão **Enviar para CPE**.

A solicitação de limpeza criada com um conjunto de comandos é enviada ao dispositivo CPE e os comandos são executados um a um. É possível visualizar o status de execução da última solicitação e seus detalhes em **Status da solicitação de limpeza mais recente**.



Status da solicitação de limpeza mais recente

Gerenciar relatórios

Relatórios gerado pelos utilitários tcpdump, iperf e OpenFlow dump. Para visualizar a tabela de relatórios em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Utilitários → Arquivos**. As informações sobre relatórios são exibidas nas seguintes colunas da tabela:

- **Tipo** é o formato do relatório.
- **Criado** é a data e a hora em que o relatório foi criado.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Baixar um relatório

Para baixar um relatório:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE do qual deseja baixar o relatório.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários → Arquivos**.

   A tabela de relatórios é exibida.

4. Clique em **Baixar** ao lado do relatório que deseja baixar.

O arquivo de relatório é salvo no dispositivo local.

Excluir um relatório

Os relatórios excluídos não podem ser restaurados.

Para excluir um relatório:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE do qual deseja excluir um relatório.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Utilitários → Arquivos**.

   A tabela de relatórios é exibida.

4. Clique em **Excluir** ao lado do relatório que deseja excluir.

5. Na janela de confirmação, clique em **Excluir**.

O relatório é excluído e não é mais exibido na tabela.

Executar tarefas em dispositivos CPE

O Kaspersky SD-WAN oferece suporte à execução de tarefas em dispositivos CPE em um horário especificado. É possível usar tags para agrupar os dispositivos CPE nos quais deseja executar uma tarefa.

Existem os seguintes tipos de tarefas:

- Scripts agendados em dispositivos CPE.
- Atualizações de firmware agendadas em dispositivos CPE selecionados manualmente e em dispositivos CPE com as tags especificadas.
- Atualização agendada das configurações do dispositivo CPE.

Quando uma tarefa é criada, ela usa o fuso horário da máquina virtual em que o orquestrador está implementado. Por exemplo, ao agendar a execução de um script em um dispositivo CPE às 14h, o script será executado às 14h no fuso horário do orquestrador, mesmo se a hora no dispositivo CPE for 18h.

Recomendamos levar em conta as seguintes considerações especiais ao gerenciar tarefas:

- Uma imprecisão de 10 segundos é considerada aceitável para o momento em que a tarefa é executada.
- Caso haja várias tarefas, elas serão executadas simultaneamente. Se o orquestrador não puder executar todas as tarefas simultaneamente, elas serão executadas na ordem em que foram criadas.
- A exclusão de um modelo de CPE automaticamente exclui todas as tarefas associadas a ele.
- A exclusão de um dispositivo CPE automaticamente exclui todas as tarefas associadas a ele.
- Excluir um script com tarefas associadas requer confirmação adicional. Ao confirmar a ação, o script será excluído e não poderá ser executado nas tarefas criadas.

- As tarefas agendadas de atualização das configurações do dispositivo CPE não estão disponíveis na seção **Programador** do menu. Só é possível agendar uma atualização na área de configurações de um dispositivo CPE individual.
- Caso haja uma tarefa agendada para alterar as configurações de um dispositivo CPE, a edição do modelo de CPE associado a esse dispositivo será bloqueada até que a tarefa relevante seja concluída ou cancelada.

As tarefas ainda não concluídas podem ser concluídas manualmente.

É possível visualizar a tabela de tarefas na seção **Programador**. As informações sobre as tarefas são exibidas nas seguintes colunas da tabela:

- **ID** é o ID da tarefa.
- **Nome** é o nome da tarefa.
- **Usuário** é o nome do usuário que criou a tarefa.
- **Criado** é a data e a hora em que a tarefa foi criada.
- **Status** é o status da tarefa:
  - **Concluído** significa que a tarefa foi concluída com êxito.
  - **Erro** significa que ocorreu um erro durante a execução da tarefa.
  - **Pendente** significa que a tarefa foi colocada no banco de dados do orquestrador e está aguardando execução.
  - **Em fila** significa que a tarefa está na fila para execução.
  - **Executando** significa que a tarefa está em execução.
- **Programada** é a data e hora em que a tarefa deve ser executada.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar uma tarefa

Para criar uma tarefa:

1. No menu, acesse a seção **Programador**.

   A tabela de tarefas agendadas é exibida.

2. Na parte superior da página, clique em **+ Tarefa**.

3. Na parte superior da barra lateral exibida, na lista **Tipo**, selecione um tipo de tarefa.

   É possível criar tarefas dos seguintes tipos no menu **Programador**:

   - Executar um script
   - Atualizar o firmware

Uma tarefa do tipo **Configurações de atualização** é criada quando um salvamento posterior das configurações é executado clicando no botão **Programação salva** na área de configurações do dispositivo CPE.

4. Especifique as configurações da tarefa. Para obter uma descrição das configurações da tarefa, consulte as seguintes instruções:

   - Scripts agendados em dispositivos CPE.
   - Agendar atualizações de firmware em dispositivos CPE com tags específicas.

5. Clique em **Criar**.

A tarefa é criada e exibida na tabela.

Executar uma tarefa manualmente

Para executar uma tarefa manualmente:

1. No menu, acesse a seção **Programador**.

   A tabela de tarefas agendadas é exibida.

2. Para executar uma única tarefa manualmente:

   a. Clique na tarefa que deseja executar manualmente.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

   b. Na parte superior da área de configurações, em **Ações**, clique em **Executar agora**.

3. Para executar várias tarefas manualmente:

   a. Marque as caixas de seleção ao lado das tarefas que deseja executar manualmente.

   b. Na parte superior da tabela, clique em **Ações** → **Executar agora**.

4. Na janela de confirmação, clique em **Executar agora**.

As tarefas são concluídas e seu status na coluna **Status** muda para **Concluído**.

Excluir uma tarefa

As tarefas excluídas não podem ser restauradas.

Para excluir uma tarefa:

1. No menu, acesse a seção **Programador**.

   A tabela de tarefas agendadas é exibida.

2. Para excluir uma única tarefa:

   a. Selecione a tarefa que deseja excluir.

      A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

   b. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

3. Para excluir várias tarefas:

   a. Marque as caixas de seleção ao lado das tarefas que deseja excluir.

   b. Na parte superior da tabela, clique em **Ações** → **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

As tarefas são excluídas e não são mais exibidas na tabela.

Verificações em dispositivos CPE

As seguintes funções são fornecidas em dispositivos CPE para garantir a integridade e a confiabilidade dos componentes críticos do sistema, inclusive o firewall:

- A verificação de integridade ajuda a garantir que arquivos executáveis e arquivos de configuração críticos, inclusive os arquivos do firewall, correspondam ao firmware lançado, além de detectar alterações não autorizadas no sistema.
- O autoteste do firewall testa a integridade do firewall.
- Bloqueio do tráfego se uma verificação falhar, a segurança da rede aumenta ainda mais para impedir a transmissão de tráfego em trânsito entre dispositivos quando algum problema for detectado.

As verificações podem ser executadas sob demanda, assim como em um agendamento; é possível configurar o agendamento em um modelo CPE ou diretamente em um dispositivo CPE.

Verificação de integridade

Essa função permite verificar automática ou manualmente a integridade dos arquivos executáveis e dos arquivos de configuração críticos, inclusive os arquivos do firewall para compará-los com as somas de verificação de referência. Ela pode detectar alterações não autorizadas e garantir que os scripts do sistema e os arquivos executáveis correspondam ao firmware lançado.

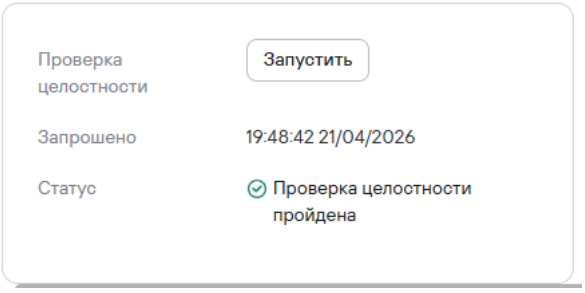
Você pode executar uma verificação por demanda ou programar uma verificação.

Execução manual de uma verificação de integridade

Para executar manualmente uma verificação de integridade:

1. No menu, acesse a seção **SD-WAN** → **CPE**.
2. Clique no dispositivo CPE no qual deseja executar a verificação.
3. No menu, selecione a seção **SD-WAN** e selecione a guia **Verificações do CPE**.
4. Abaixo de **Verificações manuais**, clique no botão **Executar** ao lado do nome da verificação.

Uma ferramenta é iniciada no dispositivo CPE, que executa a verificação e envia as informações para o registro do sistema do dispositivo CPE. A data e a hora nas quais a verificação de integridade foi iniciada são exibidas na seção **Verificações manuais**. Após a conclusão da verificação, o resultado é exibido no campo **Status**.



Resultado da verificação de integridade em um dispositivo CPE

O status e o resultado da verificação também são exibidos na área de configurações do dispositivo CPE na seção **Geral** em **Gerenciamento fora da banda**. Depois de iniciar a tarefa **Verificação de integridade**, ela assume o status **Executando**. Em seguida, dependendo do que a ferramenta retornar, o CPE envia o status sucesso ou erro ao orquestrador.

É possível verificar o status da tarefa no registro do sistema do dispositivo CPE. Para isso:

1. Abra as configurações do dispositivo CPE e acesse a seção **Informações de diagnóstico**.
2. Clique no botão **Solicitar informações de diagnóstico** e aguarde a conclusão da solicitação.
3. Na lista suspensa **Tipo**, selecione `registro de cpe`.

Caso a verificação de integridade seja bem-sucedida, o registro do sistema do dispositivo CPE incluirá uma entrada do tipo `user.info sdwan` com a mensagem `Verificação de integridade bem-sucedida`.

Registro do dispositivo CPE informando a conclusão bem-sucedida da verificação de integridade

Configuração da verificação de integridade agendada

É possível programar uma verificação de integridade em um modelo de CPE ou dispositivo CPE.

Para configurar a verificação de integridade agendada:

1. Configure a verificação de integridade agendada por meio de uma das seguintes formas:

   - Caso queira configurar a verificação de integridade agendada em um modelo CPE, acesse **SD-WAN** → seção **Modelos de CPE**, clique no modelo CPE, selecione a seção **SD-WAN** no menu lateral e selecione a guia **Verificações do CPE**.

   - Caso queira configurar a verificação de integridade agendada em um dispositivo CPE, acesse **SD-WAN** → seção **CPE**, clique no dispositivo CPE e selecione a seção **SD-WAN** no menu lateral, selecione a guia **Verificações do CPE** e ative o botão de alternância **Substituir**.

2. Abaixo de **Programar verificações**, ative o botão de alternância **Verificação de integridade**.

3. Selecione um intervalo entre as verificações na lista suspensa. As seguintes opções estão disponíveis: 1, 2, 3, 4, 6, 8 e 12 horas. O intervalo padrão é 8 horas.

4. Se necessário, ative o bloqueio do tráfego em trânsito no dispositivo CPE em caso de falha na verificação usando o botão de alternância **Bloquear o encaminhamento de tráfego se a verificação falhar**.

A ferramenta que executa a verificação e grava os resultados no registro do sistema do dispositivo CPE será iniciada no CPE em intervalos especificados.

O status e o resultado da verificação são exibidos na área de configurações do dispositivo CPE na seção **Geral** em **Gerenciamento fora da banda**. Depois de iniciar a tarefa **Verificação de integridade**, ela assume o status **Executando**. Em seguida, dependendo do que a ferramenta retornar, o CPE envia o status sucesso ou erro ao orquestrador.

Autoteste do firewall

A função permite verificar a integridade do firewall no CPE.

É possível executar manualmente a verificação ou configurar uma verificação agendada.

Execução manual de um autoteste do firewall

Para iniciar manualmente um autoteste de firewall:

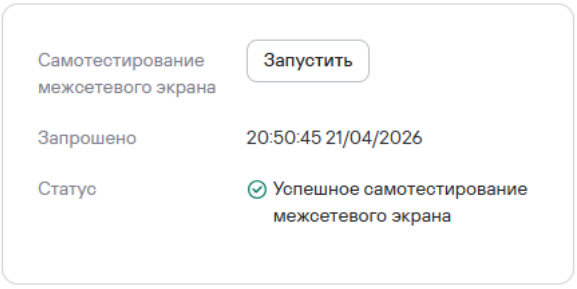
1. No menu, acesse a seção **SD-WAN** → **CPE**.

2. Clique no dispositivo CPE no qual deseja executar a verificação.

3. No menu, selecione a seção **SD-WAN** e selecione a guia **Verificações do CPE**.

4. Abaixo de **Verificações manuais**, clique no botão **Executar** ao lado do nome da verificação.

Um script é iniciado no dispositivo CPE, que executa o autoteste do firewall e envia as informações para o registro do sistema do dispositivo CPE. A data e a hora nas quais o autoteste do firewall foi iniciado são exibidas em **Verificações manuais**. Após a conclusão da verificação, o resultado é exibido no campo **Status**.



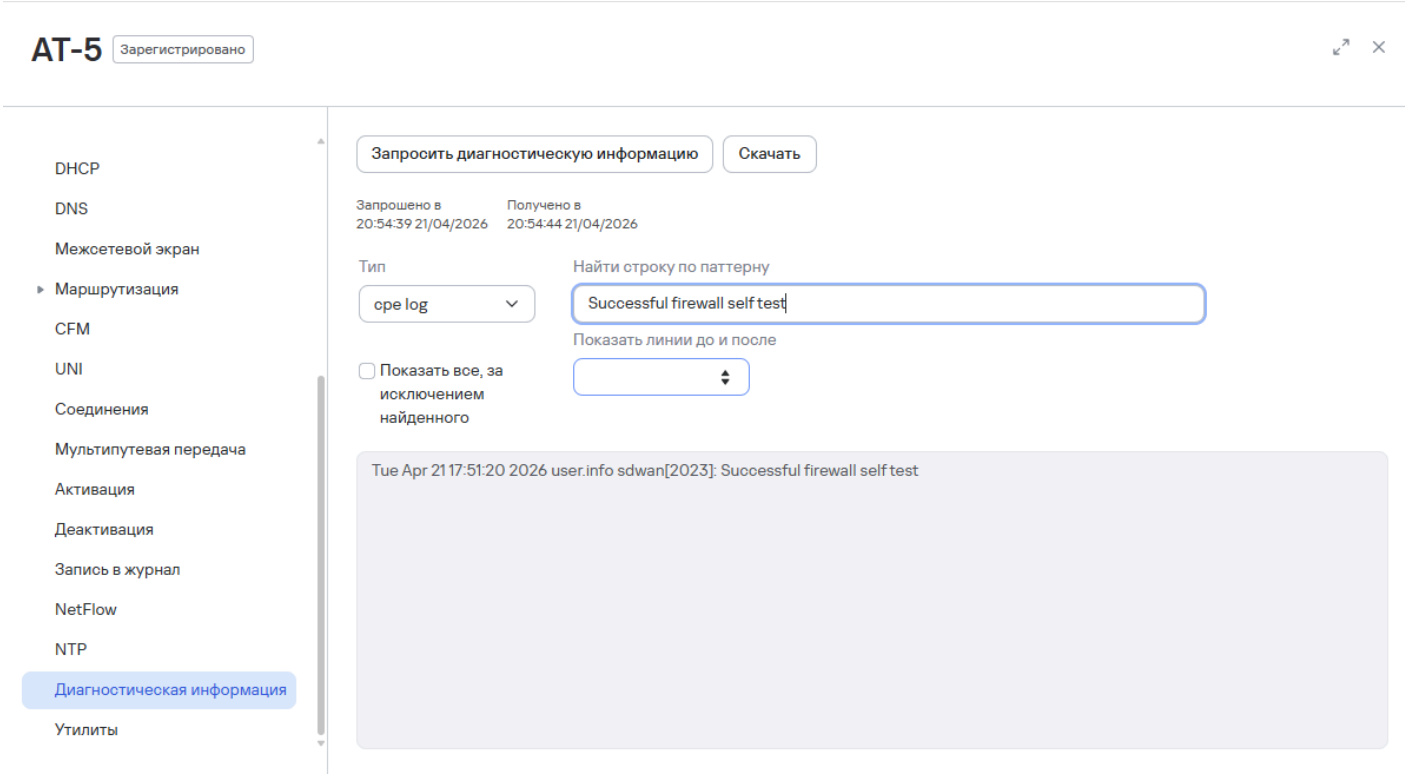
Resultado de um autoteste de firewall em um dispositivo CPE

O status e o resultado da verificação também são exibidos na área de configurações do dispositivo CPE na seção **Geral** em **Gerenciamento fora da banda**. Depois de iniciar a tarefa **Autoteste do firewall**, ela assume o status **Executando**. Em seguida, dependendo do que a ferramenta retornar, o CPE envia o status sucesso ou erro ao orquestrador.

É possível verificar o status da tarefa no registro do sistema do dispositivo CPE. Para isso:

1. Abra as configurações do dispositivo CPE e acesse a seção **Informações de diagnóstico**.
2. Clique no botão **Solicitar informações de diagnóstico** e aguarde a conclusão da solicitação.
3. Na lista suspensa **Tipo**, selecione `registro de cpe`.

Caso o autoteste do firewall tenha sido bem-sucedido, o registro de sistema do dispositivo CPE conterá um registro do tipo `user.info sdwan` com a mensagem `Autoteste do firewall bem-sucedido`.



Registro do dispositivo CPE informando a conclusão bem-sucedida do autoteste de firewall

Configuração de autoteste de firewall agendado

Você pode programar um autoteste de firewall em um modelo de CPE ou em um dispositivo CPE.

Para programar um autoteste de firewall:

1. Configure o autoteste agendado do firewall por meio de uma das seguintes formas:

   - Caso queira configurar o autoteste agendado do firewall em um modelo CPE, acesse a seção **SD-WAN → Modelos de CPE**, clique no modelo CPE, selecione a seção **SD-WAN** no menu lateral e selecione a guia **Verificações do CPE**.

   - Caso queira configurar o autoteste agendado do firewall em um dispositivo CPE, acesse **SD-WAN → seção CPE**, clique no dispositivo CPE e selecione a seção **SD-WAN** no menu lateral, selecione a guia **Verificações do CPE** e ative o botão de alternância **Substituir**.

2. Abaixo de **Programar verificações**, ative o botão de alternância **Verificação de integridade**.

3. Selecione um intervalo entre as verificações na lista suspensa. As seguintes opções estão disponíveis: 1, 2, 3, 4, 6, 8 e 12 horas. O intervalo padrão é 8 horas.

4. Se necessário, ative o bloqueio do tráfego em trânsito no dispositivo CPE em caso de falha na verificação usando o botão de alternância **Bloquear o encaminhamento de tráfego se a verificação falhar**.

O script que executa a verificação e grava os resultados no registro do sistema do dispositivo CPE será iniciado no CPE em intervalos especificados.

O status e o resultado da verificação são exibidos na área de configurações do dispositivo CPE na seção **Geral** em **Gerenciamento fora da banda**. Depois de iniciar a tarefa **Autoteste do firewall**, ela assume o status **Executando**. Em seguida, dependendo do que a ferramenta retornar, o CPE envia o status sucesso ou erro ao orquestrador.

As verificações com falha também são exibidas na guia **Problemas** do menu CPE.

Bloquear tráfego se o autoteste ou a verificação de integridade falhar

Essa função foi desenvolvida para bloquear o tráfego em trânsito (o tráfego entre as interfaces de rede e um dispositivo CPE) caso o autoteste e a verificação de integridade de arquivos e scripts críticos do sistema no dispositivo CPE falhem. Ela complementa as funções de autoteste e verificação de integridade do firewall e é configurada conjuntamente com elas. É possível ativar o bloqueio do tráfego em verificações CPE agendadas. É possível ativar ou desativar o bloqueio do tráfego em um modelo de CPE ou em um dispositivo CPE. Quando o bloqueio estiver ativado em um modelo CPE, o tráfego de trânsito será bloqueado em caso de erros de autoteste ou de verificação de integridade em todos os dispositivos CPE que usam esse modelo.

Para ativar o bloqueio do tráfego em trânsito se o autoteste ou a verificação de integridade falharem:

1. Ative o bloqueio do tráfego em trânsito por meio de uma das seguintes formas:

   - Caso queira ativar o bloqueio do tráfego em trânsito em um modelo CPE, acesse **SD-WAN** → seção **Modelos de CPE**, clique no modelo CPE, selecione a seção **SD-WAN** no menu lateral e selecione a guia **Verificações do CPE**.

   - Caso queira ativar o bloqueio do tráfego em trânsito em um dispositivo CPE, acesse **SD-WAN** → seção **CPE**, clique no dispositivo CPE e selecione a seção **SD-WAN** no menu lateral, selecione a guia **Verificações do CPE** e ative o botão de alternância **Substituir**.

2. Verifique e confirme se a verificação de integridade e o autoteste do firewall estão ativados e se o intervalo necessário entre as verificações está configurado.

   > Para ativar o bloqueio de tráfego em trânsito, ambas as verificações devem estar ativadas.

3. Ative o bloqueio do tráfego acionando o botão de alternância **Bloquear o encaminhamento de tráfego se a verificação falhar**.

   Caso tenha ativado o bloqueio do tráfego no modelo CPE, um aviso será exibido:

   Caso alguma verificação falhe, o encaminhamento de tráfego em trânsito será bloqueado em todos os dispositivos CPE com o uso deste modelo. Tem certeza de que deseja avançar

   Confirme que deseja ativar o bloqueio clicando em **Sim, prosseguir**.

4. Salve as alterações no modelo CPE ou no dispositivo CPE.

O bloqueio do tráfego em trânsito está ativado. Caso alguma das verificações falhe, o dispositivo CPE começará a bloquear o tráfego em trânsito e o orquestrador exibirá uma janela de aviso pop-up para esse dispositivo CPE. Ao mesmo tempo, a conexão entre o CPE e o orquestrador não será interrompida, o que permitirá gerenciar o dispositivo e alterar suas configurações.

Para interromper o bloqueio do tráfego em trânsito:

1. Determine a causa exata do bloqueio executando ambas as verificações manuais separadamente:

   - Verificação de integridade por demanda

   - Executar um autoteste de firewall por demanda

2. Elimine a causa:

   - Caso o problema tenha ocorrido após um autoteste do firewall, reinicie o dispositivo CPE.

   - Caso o problema ocorra após uma verificação de integridade, restaure o firmware do CPE usando o procedimento de atualização.

   - Caso tenha certeza de que o funcionamento do firewall não foi prejudicado e a verificação retornou um falso positivo, desative o botão de alternância **Bloquear o encaminhamento de tráfego se a verificação falhar** e salve as configurações do dispositivo CPE. O tráfego será desbloqueado, e após isso, será possível reativar a função de bloqueio.

Quando o tráfego em trânsito no dispositivo CPE for permitido novamente, a janela pop-up no orquestrador desaparecerá.

É possível verificar o status das verificações e do bloqueio de tráfego no registro de sistema do dispositivo CPE. Para isso:

1. Abra as configurações do dispositivo CPE e acesse a seção **Informações de diagnóstico**.
2. Clique no botão **Solicitar informações de diagnóstico** e aguarde a conclusão da solicitação.
3. Na lista suspensa **Tipo**, selecione `registro de cpe`.

   Algumas das seguintes entradas estarão presentes no registro do sistema do dispositivo CPE:

   - Tipo `user.crit.fwblock`, mensagem `Firewall self test failed. Traffic forwarding blocked`.

     O autoteste do firewall falhou. O encaminhamento de tráfego está bloqueado.

   - Tipo `user.crit.integrityblock`, mensagem `Firewall integrity check failed. Traffic forwarding blocked`.

     A verificação de integridade falhou. O encaminhamento de tráfego está bloqueado.

   - Tipo `user.info.checksuccess`, mensagem `Verification was successful`.

     As verificações foram bem-sucedidas. O tráfego em trânsito é permitido.

Auditoria de eventos de segurança

Podem ocorrer eventos no orquestrador Kaspersky SD-WAN e nos dispositivos CPE que são relevantes para a segurança da informação: autorização do usuário, modificação do modelo ou configuração do dispositivo, interação com sistemas externos etc. Esses eventos são chamados de *eventos de segurança* e requerem atenção especial dos administradores de rede. Para o registro centralizado de eventos de segurança, o Kaspersky SD-WAN permite a auditoria desses eventos. Os eventos de segurança que ocorrem no orquestrador são incluídos nos registros do contêiner do Docker no qual o orquestrador está sendo executado. Os eventos de segurança que ocorrem em dispositivos CPE são incluídos nos registros do sistema dos dispositivos. Depois de registrados, os eventos de segurança são enviados ao servidor syslog especificado no arquivo de configuração durante a implementação da solução. Para conveniência do processamento de eventos, é possível configurar um coletor SIEM externo como um servidor syslog (por exemplo, Kaspersky Unified Monitoring and Analysis Platform, doravante também referido como KUMA). Para alguns eventos de segurança, também é possível configurar quais eventos você deseja que sejam incluídos no registro de auditoria e o nível de detalhe (registrar apenas o fato do evento ou também seus detalhes).

Esta seção fornece instruções para configurar a auditoria de eventos de segurança para o orquestrador e o dispositivo CPE e para configurar um coletor KUMA externo.

Configurar o registro de eventos de segurança para auditoria

Os eventos de segurança são registrados e armazenados nos registros do orquestrador e dos dispositivos CPE. Para aproveitar todo o potencial dos registros de auditoria, você precisa configurar a exportação de eventos para um servidor syslog externo. Recomendamos usar a solução Kaspersky Unified Monitoring and Analysis Platform (KUMA) como servidor syslog.

As configurações de syslog para a exportação de registros do orquestrador devem ser especificadas no arquivo de configuração antes da implementação da solução. Se você quiser alterar as configurações, por exemplo, especificar um endereço de servidor syslog ou certificado CA diferente, será necessário alterar o arquivo de configuração e reinstalar a solução. Se você quiser usar uma conexão criptografada para o servidor syslog, precisará obter um certificado CA com antecedência

Para configurar o registro de eventos de segurança para auditoria:

1. Se quiser usar um coletor KUMA como servidor syslog:
   a. Implemente e configure o coletor KUMA conforme descrito nas instruções Configurar um coletor KUMA para processar eventos de segurança.
   b. Salve o certificado CA do servidor KUMA para usá-lo para a criptografia TLS de mensagens syslog:
      1. Abra a interface Web do KUMA.
      2. No canto inferior esquerdo da janela, clique no nome da conta de usuário e, no menu, clique em **Certificado de CA de microsserviço**.

2. Configure a exportação de registros do orquestrador para o servidor syslog no arquivo de configuração para implementação da solução:

   a. Prepare o arquivo de configuração e, nesse arquivo, insira as configurações básicas para a implementação da solução.

   b. Na seção `external.orc`, insira as seguintes configurações do servidor syslog:

   - `syslog_server_address`

     Especifique o endereço da Web do servidor syslog para o qual os contêineres Docker do orquestrador enviarão os registros. O valor é especificado no formato `<protocolo>://<endereço do host>:<número da porta>`. Você pode especificar o endereço IP ou FQDN do host como o endereço do host.

     Se você quiser que as mensagens do syslog sejam criptografadas por TLS, especifique `tcp+ ls` como protocolo.

     Exemplo:

     `tcp+tls://my-syslog-server:1514`

     > Se você estiver especificando um servidor syslog externo, por exemplo, um coletor KUMA, desative a opção de implementar um contêiner separado para o servidor syslog integrado. Para fazer isso, especifique `desativado` para a configuração `external.syslog.state`.

   - `secure_syslog`

     Especifique `true` para criptografar registros de log transmitidos ao servidor ou `false` para texto sem formatação.

     Se definido como `true`, as mensagens do syslog são enviadas via TCP com criptografia TLS. Para que o TLS funcione, você também precisa especificar o caminho para o certificado CA que assina o certificado do servidor syslog na variável `syslog_server_ca_cert_file_path`.

   - `syslog_server_ca_cert_file_path`

     Especifique o caminho absoluto para o arquivo de certificado CA que foi usado para assinar o certificado do servidor syslog. Essa configuração é necessária se você especificou `true` para a configuração `secure_syslog`.

     Se o certificado CA do servidor syslog foi emitido para um nome de domínio, para usar a criptografia TLS, você deve especificar o FQDN do servidor na configuração `syslog_server_address`. Esse nome de domínio deve ser resolvido por meio do servidor DNS especificado ao configurar o DNS no dispositivo CPE.

   - `syslog_format`

     Especifique o formato de registro a ser usado para enviar mensagens do syslog. Valores possíveis:

     - `rfc3164` para formato compatível com RFC 3164.
     - `rfc5424` para formato compatível com RFC 5424.
     - `rfc5424micro` para formato compatível com RFC 5424 usando carimbos de data e hora com precisão de microssegundos.

     Se você quiser usar um coletor KUMA como servidor syslog, especifique `rfc3164`.

3. Implementar a solução.

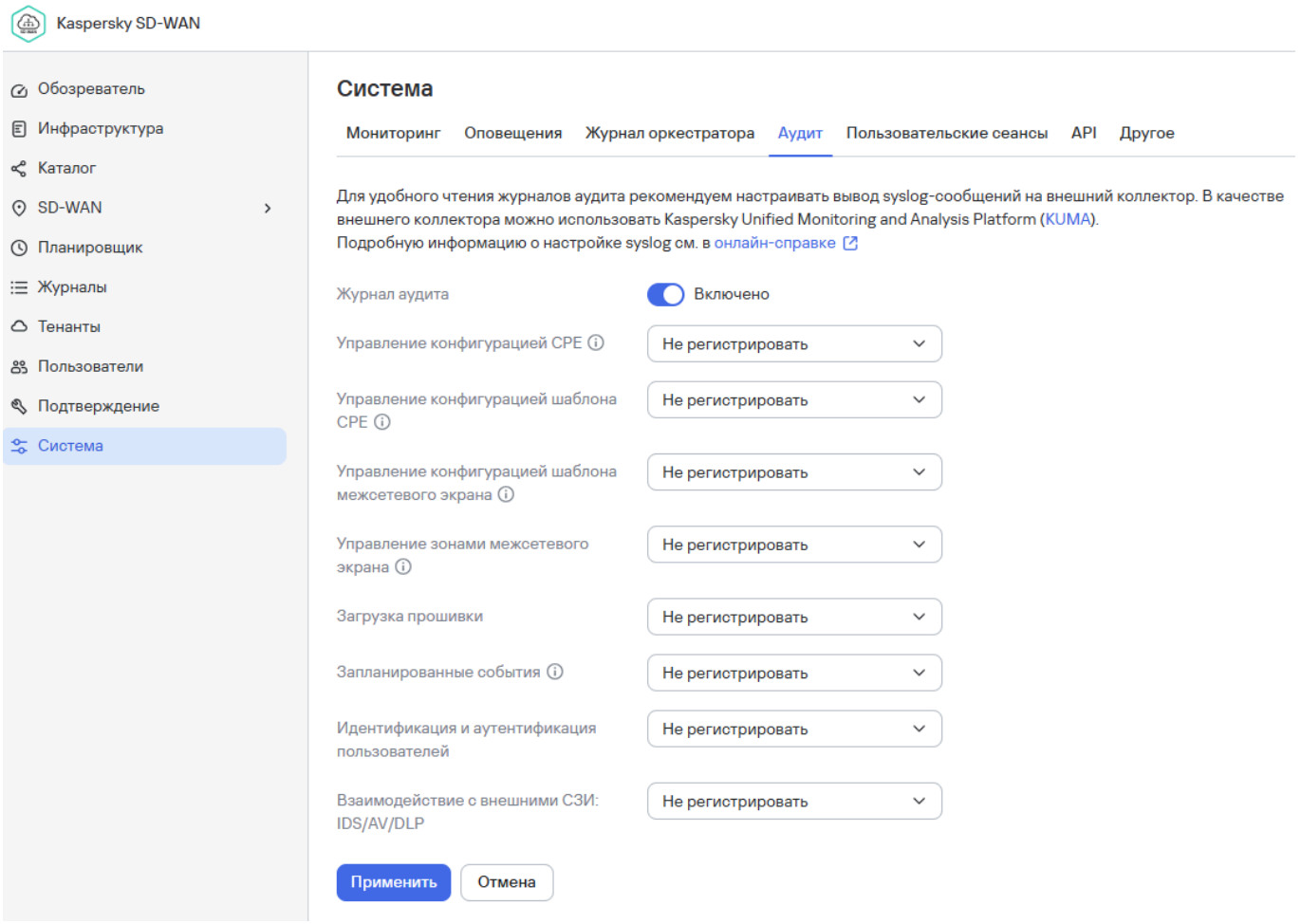
   Os contêineres do orquestrador são implementados com as configurações de servidor syslog especificadas no arquivo de configuração.

4. Faça login na interface da Web do orquestrador para gerenciar outras configurações de auditoria.

5. Selecione quais eventos de segurança do orquestrador você deseja que sejam incluídos no registro de auditoria:

   a. Acesse a seção **Sistema→Auditoria**.

      Isso abre uma lista de escopos de auditoria para os quais você pode ativar o registro dos eventos de segurança no orquestrador. Um evento de segurança ocorre quando o estado do escopo da auditoria é alterado, por exemplo, se as configurações no dispositivo ou no modelo de CPE forem alteradas ou se uma chamada de API for feita por um sistema de segurança da informação externo.



Configurar o registro de auditoria para eventos de segurança do orquestrador

   a. Ative o registro de auditoria ativando o botão de alternância **Registro de auditoria**.

      > Sempre que você ativa ou desativa essa configuração, um evento com o código `SYS-AUD` é incluído no registro de auditoria.

   b. Para cada categoria de eventos de segurança que você deseja que seja registrada, selecione o modo de registro na lista suspensa:

      - **Padrão** (registrar o fato do evento no escopo de auditoria selecionado)
      - **Estendida** (registrar informações detalhadas sobre o evento no escopo de auditoria selecionado, por exemplo, o valor antigo e o novo quando uma configuração é alterada etc. Não disponível para todas as áreas de auditoria).

c. Salve as alterações clicando no botão **Aplicar**.

Os eventos de segurança que ocorrem nos escopos de auditoria selecionados são registrados no registro de auditoria e enviados ao servidor syslog especificado no arquivo de configuração durante a implementação da solução.

Para obter uma lista detalhada de eventos de segurança que podem ser registrados no orquestrador, consulte o artigo Lista de eventos de segurança que podem ser registrados no orquestrador e dispositivos CPE.

6. Configure o servidor syslog para os registros em dispositivos CPE:

a. Na interface da Web do orquestrador, navegue até os dispositivos ou modelos de CPE nos quais você deseja configurar um servidor syslog para enviar os registros.

b. Siga as instruções Configurar registros em dispositivos CPE para gerenciar as configurações do servidor syslog. Se você quiser usar o coletor KUMA como servidor syslog, carregue o certificado CA salvo anteriormente do servidor para os dispositivos.

Os eventos de segurança que ocorrem nos dispositivos CPE serão enviados ao servidor syslog especificado.

Para obter uma lista detalhada de eventos de segurança que podem ser registrados em dispositivos CPE, consulte o artigo Lista de eventos de segurança que podem ser registrados no orquestrador e dispositivos CPE.

Lista de eventos de segurança que podem ser registrados no orquestrador e nos dispositivos CPE

A seguir, há uma lista de eventos de segurança que podem ser incluídos no registro de auditoria do orquestrador.

Lista de eventos de segurança que podem ser registrados

Código	Evento	Ação	Gravidade	Gravidade do evento KUMA	Tempo de ativação	
Registro de auditoria						
SYS-AUD	Iniciado	Subsistema de auditoria ativado	informação	baixo	Ao clicar em: Salvar	Message: Code Event: Username:$us ...], Extended: [$code ...], OrcVersion:$ SYS-AUD Started: Username:admin(te SDW-CPET, SDW-FWT, SDW-FWZ, S SYS-API], Extended: [], OrcVersion:3.0 SYS-AUD Started: Username:admin(te [SDW-CPE, SDW-CPET, SDW-FWT, S SYS-AUD Started: Username:admin(te SCH-FMWU, USR-USR, SYS-API], Ext FWZ], OrcVersion:3.0.0.release.1.cis.an
SYS-AUD	Interrompido	Subsistema de auditoria desativado	aviso	médio	Ao clicar em: Salvar	Message: Code Event: Username:$us ...], Extended: [$code ...], OrcVersion:$ SYS-AUD Stopped: Username:admin(t SDW-CPET, SDW-FWT, SDW-FWZ, S SYS-API], Extended: [], OrcVersion:3.0 SYS-AUD Stopped: Username:admin(t [SDW-CPE, SDW-CPET, SDW-FWT, S SYS-AUD Stopped: Username:admin(t SCH-FMWU, USR-USR, USR-PERM, S FWT, SDW-FWZ], OrcVersion:3.0.0.rel

SYS-AUD	Erro	Não é possível iniciar o subsistema de auditoria	aviso	médio	Imediatamente após a ocorrência	Message: Code Event: Standard: [$cc OrcVersion:$orcversion, $ErrorMessa SYS-AUD Error: Standard: [SDW-CPE SCH-FMWU, USR-USR, USR-PERM, S OrcVersion:3.0.0.release.1.cis.amd64, $ SYS-AUD Error: Standard: [], Extende OrcVersion:3.0.0.release.1.cis.amd64, $ SYS-AUD Error: Standard: [SDW-FMV Extended: [SDW-CPE, SDW-CPET, SI OrcVersion:3.0.0.release.1.cis.amd64, $
Gerenciamento de configuração do CPE						
SDW-CPE	Qualquer	Qualquer alteração em qualquer seção CPE que não se enquadre nas seções especializadas descritas abaixo.	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar SDW-CPE Any: Username:admin(tena CTenant:tenant-1, OrcVersion:3.0.0.rel
SDW - CPE	AnyError	Qualquer alteração em qualquer seção do CPE que não se enquadre nas seções especializadas descritas abaixo, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE AnyError: CPE:vCPE1, Tem
SDW-CPE	Criar	Criação de CPE	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar SDW-CPE Create: Username:admin(t Template:vCPE1, CTenant:tenant-1.
SDW-CPE	CreateError	Criação de CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE CreateError: CPE:vCPE1, T
SDW-CPE	Registro	Registro de CPE	informação	baixo	Status do CPE muda para: Ativado	Standard/Extended: Code Event: CPI SDW-CPE Registration: CPE:vCPE1, T
SDW-CPE	RegistrationError	Registro de CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE RegistrationError: CPE:vCI $ErrorMessage
SDW-CPE	Excluir	Exclusão de CPE	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar SDW-CPE Delete: Username:admin(te Template:vCPE1, TTenant:tenant-1, CT
SDW-CPE	DeleteError	Exclusão de CPE com erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE DeleteError: CPE:vCPE1, Te
SDW-CPE	Desativar	Desativação de CPE	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar SDW-CPE Disable: Username:admin(t Template:vCPE1, TTenant:tenant-1, CT
SDW-CPE	DisableError	Desativação de CPE com erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE DisableError: CPE:vCPE1, T
SDW-CPE	Ativar	Ativação de CPE	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar SDW-CPE Enable: Username:admin(te Template:vCPE1, CTenant:tenant-1
SDW-CPE	EnableError	Ativação de CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE EnableError: CPE:vCPE1, Te

SDW-CPE-GEN	FirewallTemplate	Modificação de modelos de instância do CPE	informação	baixo	Ao clicar em: Salvar	Standard: Code Event: Username:$us Template:$name, CTenant:$name, Orc SDW-CPE-GEN FirewallTemplate: Use Template:vCPE1, CTenant:tenant-1, Or Extended: Code Event: Username:$us Template:$name, CTenant:$name, Orc SDW-CPE-GEN FirewallTemplate: Use Template:vCPE1, CTenant:tenant-1, Or [Changed:Default firewall template>D
SDW-CPE-GEN	FirewallTemplateError	Modificação de modelos de instância do CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE-GEN FirewallTemplateErro $ErrorMessage
SDW-CPE-ENC	Criptografia	Alterar criptografia do link em uma instância do CPE	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar [Changed:$state], SDW-CPE-ENC Encryption: Usernam Template:vCPE1, CTenant:tenant-1, Or [Changed:enabled || disabled]
SDW-CPE-ENC	EncryptionError	Alterar criptografia do link em uma instância do CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE-ENC EncryptionError: CPE $ErrorMessage
SDW-CPE-SCR	Scripts	Executar scripts na instância do CPE	informação	baixo	Ao clicar em: Executar	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar $SriptName] SDW-CPE-SCR Scripts: Username:ac Template:vCPE1, CTenant:tenant-1, Or [Run:custom_config]
SDW-CPE-SCR	ScriptsError	Executar scripts na instância do CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE-SCR ScriptsError: CPE:vC $ErrorMessage

SDW-CPE-NET	Interface	Adicionar/remover/alterar zona/endereço IP/endereço MAC/interface de QoS na instância do CPE	informação	baixo	Ao clicar em: Salvar	Standard: Code Event: Username:$us Template:$name, CTenant:$name, Or SDW-CPE-NET Interface: Username:a Template:vCPE1, CTenant:tenant-1, O [Changed] Extended: Code Event: Username:$us Template:$name, CTenant:$name, Or Deleted || Changed: GEN || QOS: $Det SDW-CPE-NET Interface: Username:a Template:vCPE1, CTenant:tenant-1, O [Added: GEN: Zone:lan, Bridge:false, E IPv4 address:10.1.1.1, IPv4 netmask:255. broadcast:10.1.1.255, Override MAC:01: Enable QoS:false, MaxRate:1000, BE(SDW-CPE-NET Interface: Username:a Template:vCPE1, CTenant:tenant-1, O [Deleted: GEN: Zone:lan, Bridge:false, IPv4 address:10.1.1.1, IPv4 netmask:255. broadcast:10.1.1.255, Override MAC:01: Enable QoS:false, MaxRate:1000, BE(SDW-CPE-NET Interface: Username:a Template:vCPE1, CTenant:tenant-1, O [Changed: GEN: Zone: lan>lan(tenant- automatically:true>false, IPv4 input ty 10.1.1.1>10.2.2.2, IPv4 netmask: 255.0.0.0> broadcast: 10.1.1.255>10.2.2.255, Overri Generate MAC: true>false, Changed: BE(MaxR):90] Mostrar alteração de/para em Alterar Alterar de/para não é exibido em Alte imediatamente.
SDW-CPE-NET	InterfaceError	Adicionar/remover/alterar zona/interface de QoS na instância do CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CP $alias, [GEN || QoS], $ErrorMessage SDW-CPE-NET InterfaceError: CPE:v [GEN], $ErrorMessage SDW-CPE-NET InterfaceError: CPE:v [QoS], $ErrorMessage

SDW-CPE-FW	Firewall	Alterar as configurações do firewall em uma instância do CPE	informação	baixo	Ao clicar em: Salvar	Standard: Code Event: Username:$us Template:$name, CTenant:$name, Orc SDW-CPE-FW Firewall: Username:adr Template:vCPE1, CTenant:tenant-1, Or Extended: Code Event: Username:$us Template:$name, CTenant:$name, Orc GEN || RUL || ADVR || NAT || ZF || IPSET SDW-CPE-FW Firewall: Username:adr CTenant:tenant-1, OrcVersion:3.0.0.rel protection:Disable, Default INPUT act SDW-CPE-FW Firewall: Username:adr CTenant:tenant-1, OrcVersion:3.0.0.rel Action:ACCEPT, IPset:null, IPv:IPv4, Sr DstIP:3.3.3.3:4.4.4.4, Proto:icmp, + new IPset:null, IPv:IPv4, SrcZ:wan, DstZ: lan, rule), Changed: RUL: (Name:Allow-Ping DstZ:null, SrcIP:null, DstIP:null, Proto:ic SDW-CPE-FW Firewall: Username:adr CTenant:tenant-1, OrcVersion:3.0.0.rel Name:Test, Ptags:null, Table:FILTER, C rules,Start of table, DstIP:1.1.1.1, MakeA Frag:false, MarkVal:null, MarkMask:null StrAlg:BM, StrRange:1-65535, StrHEX RecentProto:SET, RecentSec:null, Rec new rule), Deleted: ADVR: (Status:On, (Status:Off, Name:ICMP ..., + new rule) SDW-CPE-FW Firewall: Username:adr CTenant:tenant-1, OrcVersion:3.0.0.rel Proto:IP, SP-DestIP:1.1.1.1, SP-SrcZone:l DestZone:wan(tenant-1), + new rule), D DestIP:1.1.1.1, SP-SrcZone:lan(tenant-1), DestZone:wan(tenant-1), + new rule), C DestIP:1.1.1.1, SP-SrcZone:lan(tenant-1), DestZone:wan(tenant-1), + new rule)] SDW-CPE-FW Firewall: Username:adr template, Owner: admin(tenant-1), Orc (From:Any zone, To:mgmt,+ new rule), Changed: ZF: (From:wan, To:lan,+ new SDW-CPE-FW Firewall: Username:adr CTenant:tenant-1, OrcVersion:3.0.0.rel Direction:Match source, Type:Set of s rule), Deleted: IPSET: (Name:test, Direc EntryList:10.1.1.[1-254]/24,20.2.2.[1-5], + Direction:Match source, Type:Set of s rule)] SDW-CPE-FW Firewall: Username:adr CTenant:tenant-1, OrcVersion:3.0.0.rel SDW-CPE-FW Firewall: Username:adr CTenant:tenant-1, OrcVersion:3.0.0.rel Input:ACCEPT, Output:ACCEPT, Forw to PMTU:false, Drop logging:false, Net ZONE: (Name:RULE2, Input:ACCEPT, C Masquerading:false, MSS clamp to PM 22.2.2.2/32, + new rule), Changed: ZON Forwarding:REJECT, Masquerading:tru Networks:11.1.1.1/32, 33.3.3.3/32, + new r PKTmark: somente os itens ativados s Alterar de/para não é exibido em Alte imediatamente.
SDW-CPE-FW	FirewallError	Alterar as configurações de firewall em uma instância CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI RUL || ADVR || NAT, ZF || IPSET || DPI || Z SDW-CPE-FW FirewallError: CPE:vCP || ADVR || NAT, ZF || IPSET || DPI || ZONE

SDW-CPE-STR	StaticRoute	Adicionar/remover/alterar configurações de roteamento estático	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar Deleted || Changed: VRF:$vrf, Destina Gateway:$gateway, Interface:$interfa Type:$type] SDW-CPET-STR StaticRoute: Userna Template:vCPE1, CTenant:tenant-1, O VRF:main/254, Destination:10.1.1.1/255. MTU:1500, AD:20, Type:unicast] SDW-CPET-STR StaticRoute: Userna Template:vCPE1, CTenant:tenant-1, O VRF:main/254, Destination:10.1.1.1/255. MTU:1500, AD:20, Type:unicast] SDW-CPET-STR StaticRoute: Userna Template:vCPE1, CTenant:tenant-1, O VRF:yellow/100, Destination:10.2.2.2/2 Metric:10, MTU:1300, AD:10, Type:black Alterar de/para não é exibido em Alte imediatamente.
SDW-CPE-STR	StaticRouteError	Adicionar/remover/alterar configurações de roteamento estático, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPE-STR StaticRoute: CPE:vCI $ErrorMessage
Gerenciamento de configuração de modelos do CPE						
SDW-CPET	Qualquer	Qualquer alteração em qualquer seção do modelo de CPE que não se enquadre nas seções especializadas descritas abaixo.	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use Template:$name, Owner:$owner, Orc SDW-CPET Any: Username:admin(ter Owner:tenant-1, OrcVersion:3.0.0.relea
SDW-CPET	AnyError	Qualquer alteração em qualquer seção do modelo de CPE que não se enquadre nas seções especializadas descritas abaixo, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: Tem SDW-CPET AnyError: Template:vCPE
SDW-CPET-ENC	Criptografia	Alterar a criptografia de link no modelo de CPE	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use Template:$name, Owner:$owner, Orc SDW-CPET-ENC Encryption: Usernar Owner:tenant-1, OrcVersion:3.0.0.relea
SDW-CPET-ENC	EncryptionError	Alterar a criptografia do link no modelo de CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: Tem SDW-CPET-ENC EncryptionError: Te
SDW-CPET-SCR	Scripts	Modificar scripts em um modelo de CPE	informação	baixo	Ao clicar em: Salvar, Executar	Standard/Extended: Code Event: Use Template:$name, Owner:$owner, Orc Changed: $SriptName] SDW-CPET-SCR Scripts: Username:a Owner:tenant-1, OrcVersion:3.0.0.relea custom_config]
SDW-CPET-SCR	ScriptsError	Modificar scripts em um modelo de CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: CPI $ErrorMessage SDW-CPET-SCR ScriptsError: Templa

SDW-CPET-NET	Interface	Adicionar/remover/alterar zona/endereço IP/endereço MAC/interface de QoS em um modelo de CPE	informação	baixo	Ao clicar em: Salvar	Standard: Code Event: Username:$us Owner:$owner, OrcVersion:$orcversio SDW-CPET-NET Interface: Username Owner:tenant-1, OrcVersion:3.0.0.relea SDW-CPET-NET Interface: Username Owner:tenant-1, OrcVersion:3.0.0.relea SDW-CPET-NET Interface: Username Owner:tenant-1, OrcVersion:3.0.0.relea Extended: Code Event: Username:$us Owner:$owner, OrcVersion:$orcversio QOS: $Detailed_change] SDW-CPET-NET Interface: Username Owner:tenant-1, OrcVersion:3.0.0.relea Bridge:false, Enable automatically:true netmask:255.0.0.0, IPv4 gateway:10.1.1.2 MAC:01:01:01:01:01:01, Generate MAC:t BE(MinR):10, BE(MaxR):100] SDW-CPET-NET Interface: Username Owner:tenant-1, OrcVersion:3.0.0.relea Bridge:false, Enable automatically:true netmask:255.0.0.0, IPv4 gateway:10.1.1.2 MAC:01:01:01:01:01:01, Generate MAC:t MaxRate:1000, BE(MinR):10, BE(MaxR) SDW-CPET-NET Interface: Username Owner:tenant-1, OrcVersion:3.0.0.relea lan>lan(tenant-1), Bridge:false>true, En Manually>From IP pool, IPv4 address: 1 IPv4 gateway: 10.1.1.254>10.2.2.254, IPv4 01:01:01:01:01:01>02:02:02:02:02:02, Ge QoS:true, MaxRate:100, BE(MinR):20, B Mostrar alteração de/para em Alterar Alterar de/para não é exibido em Alte imediatamente.
SDW-CPET-NET	InterfaceError	Adicionar/remover/alterar zona/endereço IP/endereço MAC/interface de QoS em um modelo de CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: Tem QoS], $ErrorMessage SDW-CPE-NET InterfaceError: Templ lan, [GEN], $ErrorMessage SDW-CPE-NET InterfaceError: Templ lan, [QoS], $ErrorMessage
SDW-CPET-STR	StaticRoute	Adicionar/remover/alterar configurações de rota estática em um modelo de CPE	informação	baixo	Ao clicar em: Salvar	Standard/Extended: Code Event: Use Template:$name, Owner:$owner, OrcV VRF:$vrf, Destination:$destination/$i Gateway:$gateway, Interface:$interfa Type:$type] SDW-CPET-STR StaticRoute: Userna Template:vCPE1, Owner:tenant-1, Orc VRF:main/254, Destination:10.1.1.1/255.(MTU:1500, AD:20, Type:unicast] SDW-CPET-STR StaticRoute: Userna Template:vCPE1, Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.amd64, [Gateway:10.1.1.254, Interface:lan, Metric SDW-CPET-STR StaticRoute: Userna Template:vCPE1, Owner:tenant-1, Orc VRF:yellow/100, Destination:10.2.2.2/25 Metric:10, MTU:1300, AD:10, Type:black Alterar de/para não é exibido em Alte imediatamente.
SDW-CPET-STR	StaticRouteError	Alterar as configurações de rota estática em um modelo de CPE, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: Tem SDW-CPE-STR StaticRoute: Templat

SDW-FWT	Firewall	Criar/excluir/modificar regras de modelo de firewall	informação	baixo	Ao clicar em: Salvar	Ao criar/excluir um modelo: Standard/Extended: Code Event: Use Name:$name, Owner:$owner, OrcVers SDW-FWT Firewall: Username:admin(1 template, Owner:admin(tenant-1), Orc SDW-FWT Firewall: Username:admin(1 template, Owner:admin(tenant-1), Orc Ao modificar: Standard: Code Event: Username:$us Owner:$owner, OrcVersion:$orcversio SDW-FWT Firewall: Username:admin(1 template, Owner:admin(tenant-1), Orc Extended: Code Event: Username:$us Owner:$owner, OrcVersion:$orcversio || NAT || ZF || IPSET || DPI: $Detailed_ch SDW-FWT Firewall: Username:admin(1 template, Owner:admin(tenant-1), Orc Syn-flood protection:Disable, Default SDW-FWT Firewall: Username:admin(1 template, Owner:admin(tenant-1), Orc (Name:Test, Action:ACCEPT, IPset:nul DstIP:3.3.3.3:4.4.4.4, Proto:icmp, + new IPset:null, IPv:IPv4, SrcZ:wan, DstZ: lan, rule), Changed: RUL: (Name:Allow-Ping DstZ:null, SrcIP:null, DstIP:null, Proto:ic SDW-FWT Firewall: Username:admin(1 template, Owner:admin(tenant-1), Orc (Status:On, Name:Test, Ptags:null, Tab Placement:Pre-rules,Start of table, Ds Target:ACCEPT, Frag:false, MarkVal:nu StrSrchPatt:null, StrAlg:BM, StrRange RecentName:null, RecentProto:SET, R applet,WebAsm, ..., + new rule), Delete Changed: ADVR: (Status:Off, Name:IC SDW-FWT Firewall: Username:admin(1 template, Owner: admin(tenant-1), Orc NAT:DNAT: (Name:Test, Proto:IP, SP-D SrcIP:11.1.1.1,TP-DstIP:192.1.1.1, TP-DestZo (Name:Test, Proto:IP, SP-DestIP:1.1.1.1, S DstIP:192.1.1.1, TP-DestZone:wan(tenant Proto:IP, SP-DestIP:1.1.1.1, SP-SrcZone:I DestZone:wan(tenant-1), + new rule)] SDW-FWT Firewall: Username:admin(1 template, Owner: admin(tenant-1), Orc (From:Any zone, To:mgmt,+ new rule), Changed: ZF: (From:wan, To:lan,+ new SDW-FWT Firewall: Username:admin(1 template, Owner: admin(tenant-1), Orc (Name:test, Direction:Match source, T 254]/24,20.2.2.[1-5], + new rule), Delete Type:Set of subnets, EntryList:10.1.1.[1- (Name:test, Direction:Match source, T 254]/24,20.2.2.[1-5], + new rule)] SDW-FWT Firewall: Username:admin(1 template, Owner:admin(tenant-1), Orc PKTmark:1,2,3,4] PKTmark: somente os itens ativados s Alterar de/para não é exibido em Alte imediatamente.
SDW-FWT	FirewallError	Criar/excluir/modificar regras de modelo de firewall, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: Nar NAT, ZF || IPSET || DPI], $ErrorMessage SDW-FWT FirewallError: Name:Defaul ADVR || NAT, ZF || IPSET || DPI], $Error
Gerenciamento da configuração de zonas de firewall						

SDW-FWZ	Zona	Criar/excluir/modificar regras de zona do modelo de firewall	informação	baixo	Ao clicar em: Salvar	Standard: Code Event: Username:$us Owner:$owner, OrcVersion:$orcversio SDW-FWZ Zone: Username:admin(ter Owner:admin(tenant-1), OrcVersion:3. Changed] Extended: Code Event: Username:$us Owner:$owner, OrcVersion:3.0.0.relea $Detailed_change] SDW-FWZ Zone: Username:admin(ter Owner:admin(tenant-1), OrcVersion:3. Output:ACCEPT, Forwarding:ACCEP Drop logging:false, Networks:11.1.1.1/32, SDW-FWZ Zone: Username:admin(ter Owner:admin(tenant-1), OrcVersion:3. Output:ACCEPT, Forwarding:ACCEP Drop logging:false, Networks:11.1.1.1/32, SDW-FWZ Zone: Username:admin(ter Owner:admin(tenant-1), OrcVersion:3. Output:ACCEPT, Forwarding:REJECT Drop logging:false, Networks:11.1.1.1/32, Alterar de/para não é exibido em Alte imediatamente.
SDW-FWZ	ZoneError	Criar/excluir/modificar regras de zona do modelo de firewall, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: Nar SDW-FWT ZoneError: Name:lan, Own
Fazer upload do firmware						
SDW-FMW	Firmware	Firmware enviado, verificação de integridade do pacote.	informação	informação	Ao clicar em: + Firmware	Standard/Extended: Code Event: Use [Added || Deleted: $FwName] SDW-FMW Firmware: Username:admi knaas-cpe_2.25.09.release.21.bios.amc
SDW-FMW	FirmwareError	Firmware carregado, verificação de integridade do pacote, com um erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: $Er SDW-FWT FirmwareError: $ErrorMes
Eventos agendados						
SCH-FMWU	FirmwareUpdate	Atualização de firmware no CPE	informação	baixo	Ao receber a confirmação bem-sucedida da atualização do CPE	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar SDW-FMWU FirmwareUpdate: Usern Template:vCPE1, CTenant:tenant-1, [U vkesr-m1_en-US_ru-RU.tar>knaas-cp US_ru-RU.tar]
SCH-FMWU	FirmwareUpdateError	Atualização de firmware no CPE	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: Use CPE:$name, Template:$name, CTenar SDW-FMWU FirmwareUpdate: Usern Template:vCPE1, CTenant:tenant-1, $E
SCH-UPDS	UpdateSettings	Reconfiguração do CPE programada	informação	baixo	Quando o horário programado chegar	Standard/Extended: Code Event: Use [Scheduled: CPE:$name, Time:$time] SCH-UPDS UpdateSettings: Usernam CPE:vCPE1, Time:$time]
SCH-UPDS	UpdateSettingsError	Reconfiguração de CPE programada, com erro	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: $Er SCH-UPDS UpdateSettingsError: $Er
Identificação e autenticação de usuários						
USR-USR	Autenticação	Autenticação bem-sucedida no orquestrador	informação	baixo	No login do usuário	Standard/Extended: Code Event: Use Role:$role, Account type:$type, Grou Permissions:$permissions, Permission USR-USR Authentication: Username:a Account type:LDAP, Group:admin, Pe d82e-4dfb-b7bc-414cca14abc5, Auth

USR-USR	AuthenticationError	Falha na autenticação no orquestrador	aviso	médio	Imediatamente após a ocorrência	Standard/Extended: Code Event: Use Role:$role, Account type:$type, Grou PermissionsID:$id, Authentication by USR-USR AuthenticationError: Usern Account type:LDAP, Group:admin, Pe d82e-4dfb-b7bc-414cca14abc5, Aut Se o usuário não existir: Standard/Extended: Code Event: Use by password, $ErrorMessage USR-USR AuthenticationError: Usern password, $ErrorMessage
USR-USR	UserChange	Criar/excluir/modificar funções, permissões, 2FA, senha, usuário.	informação	baixo	Ao clicar em: Salvar	Standard: Code Event: Username:$us \|\| Changed \|\| Blocked \|\| Unblocked \|\| Pa USR-USR UserChange: Username:adn USR-USR UserChange: Username:adn USR-USR UserChange: Username:adn UserTenant1] USR-USR UserChange: Username:adn USR-USR UserChange: Username:adn UserTenant1] USR-USR UserChange: Username:adn UserTenant1] USR-USR UserChange: Username:adn UserTenant1] Extended: Code Event: Username:$us || Changed || Blocked || Unblocked || Pa $Detailed_change] USR-USR UserChange: Username:adn $name, Account type:Local, Login:Use 2FA:false, Request confirmation is rec Email:boris.britva@snatch.com] USR-USR UserChange: Username:adn $name, Account type:Local, Login:Use 2FA:false, Request confirmation is rec Email:boris.britva@snatch.com] USR-USR UserChange: Username:adn $name, Account type:Local, Login:Use 2FA:false, Request confirmation is rec Email:boris.britva@snatch.com]
USR-PERM	UserPermissions	Criar/excluir/modificar privilégios de acesso.	informação	baixo	Ao clicar em: Salvar	Standard: Code Event: Username:$us || Changed: $PermissionsName] USR-PERM UserPermissions: Usernam access] USR-PERM UserPermissions: Usernam access] USR-PERM UserPermissions: Usernam access] Extended: Code Event: Username:$us || Changed: $PermissionsName, $Deta USR-PERM UserPermissions: Usernam All:Editing || Viewing || No access, Infra Domain:Editing || Viewing || No access, VIM:Editing || Viewing || No access, Co USR-PERM UserPermissions: Usernam All:Editing || Viewing || No access, Infra Domain:Editing || Viewing || No access, VIM:Editing || Viewing || No access, Co USR-PERM UserPermissions: Usernam $name, All:Editing || Viewing || No acce Domain:Editing || Viewing || No access, VIM:Editing || Viewing || No access, Co
Interação com ferramentas de segurança da informação externas: IDS/AV/DLP						

SYS-API	Call	Método de chamada da API	informação	baixo	Ao executar	Standard/Extended: Code Event API- Username:$username($tenant), srcIp: called] SYS-API Call: API-[/api/nfv/sdwan/cp 1), UserIp:127.0.0.1, Obj:[..]
SYS-API	CallComplete	Método de chamada da API concluído	informação	baixo	Ao executar	Standard/Extended: Code Event API- Username:$username($tenant), srcIp: called], Ret: [return code] SYS-API CallComplete: API-[/api/nfv [GET]: Username:admin(tenant-1), Use

A seguir: uma lista de eventos de segurança que podem ser incluídos no registro de auditoria de um dispositivo CPE.

Tabela 2. Lista de eventos de segurança que podem ser registrados em dispositivos CPE

Facility.Severity (Código)	Aplicativo	Evento	Ação	Gravidade do evento KUMA	Tempo de ativação	Mensagem
Identificação e autenticação de usuários						
authpriv.info (10.6)	dropbear	Conexão secundária a partir de	Autenticação no dispositivo	baixo	Ao executar	Tue Oct 21 07:43:34 2025 authpriv.info dropbear[160 Child connection from 172.17.9.200:60634 Tue Oct 21 07:43:34 2025 authpriv.info dropbear[160 Exit before auth from <172.17.9.200:60634>: Exited normally Tue Oct 21 07:43:42 2025 authpriv.info dropbear[1617 Child connection from 172.17.9.200:56364
authpriv.info (10.6)	dropbear	Máximo de tentativas de autenticação atingidas	Autenticação no dispositivo	alto	Ao executar	Tue Oct 21 07:46:54 2025 authpriv.info dropbear[184 Exit before auth from <172.17.9.200:57270>: (user 'root fails): Max auth tries reached - user 'root'
authpriv.notice (10.5)	dropbear	Autenticação de senha bem-sucedida	Autenticação no dispositivo	baixo	Ao executar	Tue Oct 21 07:43:45 2025 authpriv.notice dropbear[16170]: Password auth succeeded for 'root' from 172.17.9.200:56364
authpriv.warn (10.4)	dropbear	Tentativa de senha incorreta	Autenticação no dispositivo	médio	Ao executar	Tue Oct 21 07:46:52 2025 authpriv.warn dropbear[184 Bad password attempt for 'root' from 172.17.9.200:572 Tue Oct 21 07:46:53 2025 authpriv.warn dropbear[184 Bad password attempt for 'root' from 172.17.9.200:572 Tue Oct 21 07:46:54 2025 authpriv.warn dropbear[184 Bad password attempt for 'root' from 172.17.9.200:572
Gerenciamento de configuração do firewall/CPE						
user.info (1.6)	sdwan-oob	Recebido e executar tarefa de firewall	Regras de firewall alteradas	baixo	Ao executar	Wed Nov 12 09:01:04 2025 user.info sdwan-oob: Recieved and execute task firewall id abb0629b-757e-423a-b71d-2e330ef11b8b executor oob_firewall Wed Nov 12 09:01:05 2025 user.info sdwan-oob: Task firewall id abb0629b-757e-423a-b71d-2e330ef11b8b executor oob_firewall completed
user.crit (1.2)	firewall	Firewall interrompido	Serviço de firewall interrompido	crítico	Ao executar	Thu Oct 23 13:04:40 2025 user.crit firewall: Firewall stopped
user.info (1.6)	firewall	Firewall iniciado	Serviço de firewall iniciado	baixo	Ao executar	Thu Oct 23 13:04:44 2025 user.info firewall: Firewall started
user.warn (1.4)	firewall	Firewall reiniciado	Serviço de firewall reiniciado	médio	Ao executar	Thu Oct 23 13:04:55 2025 user.warn firewall: Firewall restarted
user.warn (1.4)	firewall	Firewall recarregado	Serviço de firewall recarregado	médio	Ao executar	Thu Oct 23 13:04:59 2025 user.warn firewall: Firewall reloaded
Registro de filtragem/transmissão de tráfego no firewall						

kern.info (0.6)	kernel	FW-AUD	Auditoria de desempenho do firewall	baixo	Ao executar	Sat Nov 1 11:54:41 2025 kern.info kernel: [337220.695(FW-AUD= OUT=eth0 SRC=172.17.9.221 DST=172.17.9.203 LEN=299 TOS=0x00 PREC=0xC0 TTL=64 ID=39548 [PROTO=TCP SPT=54280 DPT=6653 WINDOW=3219 RES=0x00 ACK PSH URGP=0 MARK=0x1f4
Verificação de integridade do firewall/CPE						
user.info (1.6)	sdwan	Verificação de integridade bem-sucedida	Integridade não violada	baixo	Ao executar	Thu Apr 9 11:45:44 2026 user.info sdwan[31284]: Integ check successful
user.crit (1.2)	sdwan	Falha na verificação de integridade	Violação da integridade do arquivo	crítico	Ao executar	Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]: Integ check failed
user.crit (1.2)	sdwan	Incompatibilidade com verificador 'Gost2012'. Reason: File <$file>	Violação da integridade do arquivo	crítico	Ao executar	Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]: Verification mismatch with 'Gost2012' checker. Reasc File "/usr/sbin/sdwan" has unexpected hash Vmd5sJ2GwLK35woBdeivZ1NAtsXlZNDBga2W4LH5 != expected ttDJAQ1XW+UmYx4RdVru2YFWR2Al1YzG9BO4Nvx2
user.crit (1.2)	sdwan	A verificação de integridade falhou. Encaminhamento de tráfego bloqueado	Tráfego bloqueado	crítico	Ao executar	Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]: Integ check failed. Encaminhamento de tráfego bloqueado
user.info (1.6)	sdwan	Autoteste do firewall bem-sucedido	Teste de firewall bem-sucedido	informação	Ao executar	Thu Feb 26 12:15:48 2026 user.info sdwan[7241]: Successful firewall self test
user.crit (1.2)	sdwan	Falha no autoteste do firewall	Teste de firewall malsucedido	crítico	Ao executar	Thu Feb 26 13:27:06 2026 user.crit sdwan[30591]: Fire self test failed
Conectar dispositivos USB						
kern.info (0.6)	kernel	usb	Dispositivo USB conectado	médio	Ao executar	Tue Feb 10 08:08:34 2026 kern.info kernel: [136.3260 usb 2-2: new SuperSpeed Gen 1 USB device number using xhci_hcd Tue Feb 10 08:08:34 2026 kern.info kernel: [136.3720 usb-storage 2-2:1.0: USB Mass Storage device detec Tue Feb 10 08:08:34 2026 kern.info kernel: [136.3724 scsi host2: usb-storage 2
kern.info (0.6)	kernel	mounted	Dispositivo USB montado	alto	Ao executar	Tue Feb 10 08:09:30 2026 kern.info kernel: [191.87720 EXT4-fs (sdb2): mounted filesystem with ordered dat mode. Opts: (null)
Mudança de horário						
daemon.warn (3.4)	chronyd	time jump detected	Mudança de horário	médio	Ao executar	Tue Feb 10 08:04:13 2026 daemon.warn chronyd[442 Backward time jump detected! Tue Feb 10 08:04:13 2026 daemon.info chronyd[4428 Can't synchronise: no selectable sources Tue Feb 10 08:07:27 2026 daemon.info chronyd[4428 Selected source 45.141.102.99 (0.pool.ntp.org) Tue Feb 10 08:07:27 2026 daemon.warn chronyd[442 System clock wrong by 77.778277 seconds Tue Feb 10 08:56:20 2026 daemon.warn chronyd[835 Forward time jump detected! Tue Feb 10 08:56:20 2026 daemon.info chronyd[8350 Can't synchronise: no selectable sources Tue Feb 10 08:58:33 2026 daemon.info chronyd[8350 Selected source 89.109.251.24 (0.pool.ntp.org) Tue Feb 10 08:58:33 2026 daemon.warn chronyd[835 System clock wrong by -53.343945 seconds

Intervalos de endereços IP e sub-redes para dispositivos CPE

É possível criar intervalos de endereços IP e sub-redes para atribuir endereços IPv4 de forma centralizada ao criar ou editar interfaces de rede de dispositivos CPE. Também é possível usar intervalos de endereços IP para atribuir endereços IPv4 de forma centralizada a IDs de roteador de dispositivos CPE ao especificar as configurações básicas de BGP.

Gerenciar intervalos de endereços IP

Para visualizar a tabela de intervalos de endereços IP, vá para a seção **SD-WAN → IPAM**. A guia **Pools de endereço IP** é selecionada por padrão. As informações sobre os intervalos de endereços IP são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do intervalo de endereços IP.
- **CIDR** é o prefixo IPv4 da sub-rede na qual o intervalo de endereços IP está localizado.
- **Intervalo de IPs** indica os valores inicial e final do intervalo de endereços IP.
- **Utilização** é o número de endereços IP no intervalo que foram atribuídos a interfaces de rede ou IDs de roteador de dispositivos CPE.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um intervalo de endereços IP

Para criar um intervalo de endereços IP:

1. No menu, acesse a seção **SD-WAN → IPAM**.

   Por padrão, é selecionada a guia **Pools de endereço IP**, que exibe uma tabela de intervalos de endereços IP.

2. Na parte superior da página, clique em **+ Pool de endereço IP**.
3. Na janela aberta, no campo **Nome**, insira o nome do intervalo de endereços IP. O comprimento máximo do nome é de 32 caracteres.
4. No campo **CIDR**, insira o prefixo IPv4 da sub-rede na qual o intervalo de endereços IP está localizado.

5. Especifique um intervalo de endereços IP. Para isso, em **Intervalo de IPs**, clique em **+ Adicionar** e insira os valores inicial e final do intervalo de endereços IP.

   O intervalo de endereços IP é especificado e exibido na seção **Intervalo de IPs**. É possível especificar diversos intervalos de endereços IP ou excluir intervalos de endereços IP. Para excluir um intervalo de endereços IP, clique no ícone de exclusão ✕ ao lado dele.

6. Clique em **Criar**.

O intervalo de endereços IP é criado e exibido na tabela.

Editar um intervalo de endereços IP

Para alterar um intervalo de endereços IP:

1. No menu, acesse a seção **SD-WAN → IPAM**.

   Por padrão, é selecionada a guia **Pools de endereço IP**, que exibe uma tabela de intervalos de endereços IP.

2. Clique no intervalo de endereços IP que deseja editar.

3. Na janela aberta, se necessário, edite o nome e o prefixo IPv4 da sub-rede que contém o intervalo de endereços IP e especifique ou exclua os intervalos de endereços IP.

4. Na parte superior da área de configurações, clique em **Salvar**.

O intervalo de endereços IP é modificado e atualizado na tabela.

Visualizar o uso de um intervalo de endereços IP

Se necessário, é possível verificar quais modelos de CPE e dispositivos CPE estão usando um intervalo de endereços IP. Por exemplo, se um intervalo de endereços IP estiver em uso, ele não pode ser excluído. Também é possível visualizar informações sobre endereços IP que foram atribuídos a partir do intervalo de endereços IP.

Para ver se um intervalo de endereços IP está sendo usado:

1. No menu, vá para a seção **SD-WAN → IPAM**.

   Por padrão, é selecionada a guia **Pools de endereço IP**, que exibe uma tabela de intervalos de endereços IP.

2. Clique no intervalo de endereços IP cujas informações de uso deseja visualizar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configuração**, que exibe as configurações do intervalo de endereços IP.

3. Visualize o uso do intervalo de endereços IP de uma das seguintes formas:

   - Para verificar os dispositivos CPE que estão usando um intervalo de endereços IP, selecione a guia **Utilização → CPE**.

     Uma lista de dispositivos CPE que estão usando o intervalo de endereços IP é exibida.

- Para verificar os modelos de CPE que estão usando um intervalo de endereços IP, selecione a guia **Utilização** → **Modelo**.

  Uma lista de modelos de CPE que estão usando o intervalo de endereços IP é exibida.

4. Para visualizar informações sobre endereços IP que foram atribuídos a partir do intervalo de endereços IP, selecione a guia **Concessões**.

   Uma tabela de endereços IP atribuídos a partir do intervalo de endereços IP é exibida. As informações sobre os endereços IP são exibidas nas seguintes colunas da tabela:

   - **Endereço IP** é o endereço IP atribuído a partir do intervalo de endereços IP.
   - **CPE** é o dispositivo CPE ao qual o endereço IP está atribuído.
   - **Tipo** indica se o endereço IP está atribuído a uma interface de rede ou ID de roteador de um dispositivo CPE.
   - **Nome** é o nome da interface de rede à qual o endereço IP está atribuído. Se um endereço IP tiver sido atribuído ao ID do roteador do dispositivo CPE, nenhum valor é exibido nessa coluna.
   - **Locatário** é o locatário ao qual o dispositivo CPE foi adicionado.

As ações que podem ser executadas com as listas e a tabela são descritas nas instruções Gerenciar tabelas de componentes da solução.

Excluir intervalos de endereços IP

Um intervalo de endereços IP não pode ser excluído se estiver sendo usado por pelo menos um modelo de CPE ou dispositivo CPE. Para remover um intervalo de endereços IP usado por modelos de CPE ou dispositivos CPE, primeiro remova o intervalo de endereços IP das configurações da interface de rede e das configurações do BGP. É possível verificar quais modelos de CPE e dispositivos CPE estão usando um intervalo de endereços IP.

Os intervalos de endereços IP excluídos não podem ser restaurados.

Para excluir intervalos de endereços IP:

1. No menu, acesse a seção **SD-WAN** → **IPAM**.

   Por padrão, é selecionada a guia **Pools de endereço IP**, que exibe uma tabela de intervalos de endereços IP.

2. Para excluir um único intervalo de endereços IP:

   a. Clique no intervalo de endereços IP que deseja excluir.

      A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⩓. Por padrão, é selecionada a guia **Configuração**, que exibe as configurações do intervalo de endereços IP.

   b. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

3. Para excluir vários intervalos de endereços IP:

   a. Marque as caixas de seleção ao lado dos intervalo de endereços IP que deseja excluir.

   b. Na parte superior da tabela, clique em **Ações** → **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

Os intervalos de endereços IP são excluídos e não são mais exibidos na tabela.

Gerenciar intervalos de sub-redes

Para visualizar a tabela de intervalos de sub-rede, vá para a seção **SD-WAN→ IPAM** e selecione a guia **Pools de sub-rede**. As informações sobre intervalos de sub-redes são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do intervalo da sub-rede.
- **CIDR** é o prefixo IPv4 do intervalo de sub-redes.
- **Utilização** é o número de sub-redes que foram atribuídas às interfaces de rede.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um intervalo de sub-redes

Para criar um intervalo de sub-redes:

1. No menu, acesse a seção **SD-WAN** → **IPAM**.

   Por padrão, é selecionada a guia **Pools de endereço IP**, que exibe uma tabela de intervalos de endereços IP.

2. Selecione a guia **Pools de sub-rede**.

   Uma tabela de intervalos de sub-redes é exibida.

3. Na parte superior da página, clique em **+ Pool de sub-rede**.

4. Na janela aberta, no campo **Nome**, insira o nome do intervalo de sub-redes. O comprimento máximo do nome é de 32 caracteres.

5. No campo **CIDR de base**, insira o prefixo IPv4 do intervalo de sub-redes.

6. No campo **Subprefixo**, insira o comprimento do prefixo de sub-rede IPv4 no intervalo de sub-redes. Intervalo de valores: 0 a 32.

7. Clique em **Criar**.

O intervalo de sub-redes é criado e exibido na tabela.

Editar um intervalo de sub-redes

Para editar um intervalo de sub-redes:

1. No menu, vá para a seção **SD-WAN → IPAM**.

   Por padrão, é selecionada a guia **Pools de endereço IP**, que exibe uma tabela de intervalos de endereços IP.

2. Selecione a guia **Pools de sub-rede**.

   Uma tabela de intervalos de sub-redes é exibida.

3. Clique no intervalo de sub-redes que deseja editar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃. Por padrão, é selecionada a guia **Configuração**, que exibe as configurações do intervalo de sub-redes.

4. Na janela aberta, se necessário, edite as seguintes configurações:

   - Nome do intervalo de sub-redes
   - Prefixo IPv4 do intervalo de sub-redes
   - Comprimento do prefixo IPv4 das sub-redes no intervalo de sub-redes

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do intervalo de sub-redes.

O intervalo de sub-redes é modificado e atualizado na tabela.

Visualizar o uso de um intervalo de sub-redes

Se necessário, é possível verificar quais modelos de CPE e dispositivos CPE estão usando um intervalo de sub-redes. Por exemplo, se um intervalo de sub-redes estiver em uso, ele não pode ser excluído. Também é possível visualizar informações sobre sub-redes que foram atribuídas a partir do intervalo de sub-redes.

Para ver se um intervalo de sub-redes está sendo usado:

1. No menu, acesse a seção **SD-WAN → IPAM**.

   Por padrão, é selecionada a guia **Pools de endereço IP**, que exibe uma tabela de intervalos de endereços IP.

2. Selecione a guia **Pools de sub-rede**.

   Uma tabela de intervalos de sub-redes é exibida.

3. Clique no intervalo de sub-redes cujas informações de uso deseja visualizar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃. Por padrão, é selecionada a guia **Configuração**, que exibe as configurações do intervalo de sub-redes.

4. Visualize o uso do intervalo de sub-redes de uma das seguintes formas:

   - Para verificar os dispositivos CPE que estão usando um intervalo de sub-redes, selecione a guia **Utilização → CPE**.

     Uma lista de dispositivos CPE que estão usando o intervalo de sub-redes é exibida.

   - Para verificar os modelos de CPE que estão usando um intervalo de sub-redes, selecione a guia **Utilização → Modelo**.

     Uma lista de modelos de CPE que estão usando o intervalo de sub-redes é exibida.

5. Para visualizar informações sobre sub-redes que foram atribuídas a partir do intervalo de sub-redes, selecione a guia **Concessões**.

   Uma tabela de sub-redes atribuídas a partir do intervalo de sub-redes é exibida. As informações sobre sub-redes são exibidas nas seguintes colunas da tabela:

   - **CIDR** é o prefixo IPv4 da sub-rede que foi atribuída a partir do intervalo de sub-redes.
   - **CPE** é o dispositivo CPE ao qual um endereço IPv4 da sub-rede é atribuído.
   - **Nome** é o nome da interface de rede à qual um endereço IPv4 da sub-rede é atribuído.
   - **Locatário** é o locatário ao qual o dispositivo CPE foi adicionado.

As ações que podem ser executadas com as listas e a tabela são descritas nas instruções Gerenciar tabelas de componentes da solução.

Excluir intervalos de sub-redes

Uma sub-rede não pode ser excluída se estiver sendo usada por pelo menos um modelo de CPE ou dispositivo CPE. Para remover um intervalo de sub-redes usado por modelos de CPE ou dispositivos CPE, primeiro remova o intervalo de sub-redes das configurações da interface de rede e das configurações do BGP. É possível verificar quais modelos de CPE e dispositivos CPE estão usando um intervalo de sub-redes.

Os intervalos de sub-redes excluídos não podem ser restaurados.

Para excluir intervalos de sub-redes:

1. No menu, acesse a seção **SD-WAN → IPAM**.

   Por padrão, é selecionada a guia **Pools de endereço IP**, que exibe uma tabela de intervalos de endereços IP.

2. Selecione a guia **Pools de sub-rede**.

   Uma tabela de intervalos de sub-redes é exibida.

3. Para excluir um único intervalo de sub-redes:

   a. Clique no intervalo de sub-redes que deseja excluir.

      A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configuração**, que exibe as configurações do intervalo de sub-redes.

   b. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

4. Para excluir vários intervalos de sub-redes:

    a. Marque as caixas de seleção ao lado dos intervalos de sub-redes que deseja excluir.

    b. Na parte superior da tabela, clique em **Ações** → **Excluir**.

5. Na janela de confirmação, clique em **Excluir**.

Os intervalos de sub-redes são excluídos e não são mais exibidos na tabela.

Gerenciar o firewall

Há duas abordagens principais para filtrar o tráfego:

- O filtro de tráfego de rede clássico
- O firewall baseado em zona

O **modelo de filtro de tráfego de rede** oferece um nível baixo de abstração: as regras definem o comportamento de cada pacote individual. A sintaxe de um filtro de pacotes, como iptables, vincula *regras* a *cadeias* que formam *tabelas*. Cada pacote passa por várias tabelas e, em cada tabela, passa por uma das cadeias padrão. O fato de uma regra pertencer a uma tabela (filter, nat, mangle, raw, etc.) geralmente é determinado pelo tipo de ação a ser executada. As regras geralmente estão vinculadas a interfaces individuais (de entrada ou de saída). Para cobrir interfaces adicionais, uma regra deve ser copiada e modificada.

O **modelo de firewall baseado em zona** oferece um alto nível de abstração: as zonas atuam como contêineres para interfaces e uma política (um conjunto de regras) define a interação entre as zonas.

As zonas são grupos lógicos de interfaces que a política de segurança considera do mesmo tipo.

Uma política (conjunto de regras) define como as zonas interagem umas com as outras. As regras são escritas apenas uma vez para um par de zonas (Zona A ↔ Zona B) e são automaticamente aplicadas a todas as interfaces pertencentes a essas zonas. O tráfego é classificado por protocolo e endereço e comparado com a política entre as duas zonas.

Assim, o conceito de **firewall baseado em zona** corresponde às tabelas e às cadeias de um **filtro de pacotes** iptables somente no nível de processamento de pacotes de nível básico. O firewall baseado em zona adiciona agrupamento lógico e política centralizada ao filtro de pacotes, tornando a administração mais escalável, menos suscetível a erros e mais fácil de reutilizar.

O Kaspersky SD-WAN implementa ambas as abordagens para filtrar pacotes de tráfego em dispositivos CPE.

O firewall pode aceitar, descartar ou rejeitar pacotes de tráfego. Se um pacote de tráfego for rejeitado, o remetente recebe uma mensagem `icmp-reject`. O firewall pode aplicar cada ação a pacotes de tráfego de entrada e de saída, bem como a pacotes de tráfego retransmitidos entre interfaces de rede e sub-redes de dispositivos CPE. Ao especificar as configurações básicas do firewall, defina as ações padrão que o firewall executa com pacotes de tráfego.

Os modelos de firewall são usados para o gerenciamento centralizado das configurações de firewall em dispositivos CPE. Para evitar gerenciar as configurações em cada dispositivo CPE individualmente, você pode especificar as configurações de filtragem em um modelo de firewall e, em seguida, aplicá-lo aos dispositivos CPE ao adicionar ou registrar dispositivos CPE manualmente. Ao editar uma configuração em um modelo de firewall, a configuração é automaticamente modificada em todos os dispositivos CPE que estiverem usando o modelo. Ao editar uma configuração no dispositivo CPE, essa configuração se torna independente do modelo de firewall e, caso seja modificada no modelo de firewall, permanece inalterada no dispositivo CPE.

Zonas de firewall

É possível adicionar interfaces de rede e sub-redes a uma zona de firewall (doravante também referida como 'zona') para receber, descartar ou rejeitar pacotes de tráfego transmitidos por meio dessas interfaces de rede e sub-redes. Ao criar ou editar uma zona de firewall, especifique as ações a serem executadas com pacotes de tráfego e, se necessário, adicione sub-redes. É possível adicionar interfaces de rede a uma zona de firewall ao criar ou editar uma interface de rede.

Para permitir a transmissão de pacotes de tráfego de uma zona de firewall para outra, será necessário criar um encaminhamento. Ao criar um encaminhamento, especifique as zonas de firewall de entrada e de saída.

É possível criar zonas de firewall comuns que vários dispositivos CPE podem usar, bem como zonas de firewall em um único dispositivo CPE.

Regras de firewall padrão (firewall baseado em zona)

É possível criar regras padrão de firewall para aceitar, descartar ou rejeitar pacotes de tráfego com base nos critérios especificados. Por exemplo, uma regra de firewall que rejeite pacotes de tráfego com uma zona de firewall de origem especificada.

Para especificar os mesmos endereços IP ou sub-redes em várias regras de firewall, crie um conjunto de IPs. Ao criar um conjunto de IPs, é necessário especificar se os endereços IP e as sub-redes pertencem à origem ou ao destino. É possível especificar o conjunto de IPs criado ao criar ou modificar uma regra de firewall.

Quando um pacote de tráfego é encaminhado para um dispositivo CPE, a ação especificada nas configurações de uma das regras de firewall é executada no pacote de tráfego. Se nenhuma das regras de firewall puder ser aplicada, a ação especificada nas configurações da zona de firewall para a qual o pacote foi encaminhado é aplicada ao pacote de tráfego. Se o pacote de tráfego não tiver sido encaminhado para nenhuma das zonas de firewall, a ação padrão definida ao especificar as configurações básicas do firewall será aplicada ao pacote de tráfego.

Regras de firewall avançadas (filtro de pacotes clássico)

As regras avançadas de firewall permitem um processamento de pacotes mais flexível e granular do que as regras padrão, usando critérios adicionais de correspondência e ações aplicáveis aos pacotes. Você pode usar regras avançadas de firewall quando as regras padrão não forem suficientes, por exemplo, para corresponder pacotes com base em critérios adicionais ou executar ações não padrão. Por exemplo, se você configurou várias regras de firewall por zona e interface em um CPE, mas precisa ocultar a estrutura da rede na qual o CPE está localizado, é possível criar uma regra avançada adicional para descartar pacotes com códigos ICMP que possam ser usados para reconhecimento da topologia da rede e posicionar essa regra avançada em uma etapa inicial do processamento do tráfego.

De acordo com o modelo de filtro de pacotes clássico, as regras de firewall avançadas podem ser agrupadas em dois grupos. O primeiro grupo permite adicionar novas regras antes das regras existentes (tais regras avançadas são chamadas de pré-regras) ou no segundo grupo que segue as regras existentes (tais regras avançadas são chamadas de pós-regras). A ordem das regras determina a prioridade do processamento do tráfego. Ter dois grupos de regras de processamento em cada cadeia de cada tabela permite alterar com flexibilidade a lógica de processamento do tráfego de um grupo individual de regras sem quebrar a lógica e a ordem de processamento do tráfego em um grupo de regras já configurado.

As regras de firewall baseado em zona são implementadas no filtro de pacotes clássico usando cadeias personalizadas. Portanto, as regras padrão criadas de acordo com a abordagem baseada em zona e as regras avançadas criadas na sintaxe do filtro de pacotes clássico não se cruzam nem afetam umas às outras.

Conversão de endereços de rede

Um firewall baseado em zonas é compatível com os seguintes mecanismos de tradução de endereços de rede (NAT):

- As regras de DNAT podem substituir os seguintes componentes dos pacotes de tráfego pelos valores especificados:
  - Endereços IP ou prefixos de destino
  - Zonas de firewall de destino
  - Portas de destino (Conversão de endereços de porta, PAT)
- As regras de SNAT podem substituir endereços IP de origem ou prefixos de pacotes de tráfego pelos valores especificados.

As regras de DNAT e SNAT são aplicadas a pacotes de tráfego com base nos critérios especificados. Por exemplo, é possível criar uma regra de DNAT que substitui o endereço IP de destino dos pacotes de tráfego TCP.

Na sintaxe do filtro de pacotes clássico, a tradução de endereços de rede é descrita usando as ações correspondentes na tabela mangle nas regras avançadas.

Gerenciar zonas de firewall

Para visualizar a tabela de zonas de firewall comuns ou a tabela de zonas de firewall no dispositivo CPE:

- Para visualizar a tabela de zonas de firewall comuns, vá para a seção **SD-WAN→ Zonas de firewall** do menu.
- Para visualizar a tabela de zonas de firewall em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Firewall → Zonas**.

As seguintes zonas de firewall são criadas por padrão:

- **wan** (zona de firewall WAN) é a zona de firewall para interfaces de rede conectadas à WAN, por exemplo, à Internet ou à rede do provedor de serviços. O mascaramento é ativado nas configurações da zona WAN do firewall para substituir o endereço IP de origem dos pacotes de tráfego de saída da zona do firewall pelo endereço IP atribuído à interface de rede de saída.
- **lan** (zona de firewall LAN) é a zona de firewall para interfaces de rede conectadas à LAN.
- **mgmt** (zona de firewall de gerenciamento) é a zona de firewall para a interface de rede usada para o monitoramento passivo do dispositivo CPE pelo sistema de monitoramento Zabbix, bem como para a conexão SSH do orquestrador ao dispositivo CPE.

Não é possível excluir as zonas de firewall padrão ou criar zonas de firewall com os mesmos nomes.

Ao fazer o upgrade do Kaspersky SD-WAN da versão 2.1 para a 2.2, as seguintes alterações são feitas nas configurações de todos os modelos de CPE:

- As interfaces de rede **sdwan<0–4>** são automaticamente adicionadas à zona WAN do firewall.
- As interfaces de rede **lan**, **br-lan** e **overlay** são automaticamente adicionadas à zona LAN do firewall.

As informações sobre as zonas de firewall comuns são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da zona de firewall.
- **Utilização** indica se a zona de firewall está sendo usada por modelos de firewall, modelos de CPE e dispositivos CPE:
  - **Sim**.
  - **Não**.
- **Autor** é o nome do usuário que criou a zona de firewall.
- **Criado** é a data e hora em que a zona de firewall foi criada.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

As informações sobre zonas de firewall no dispositivo CPE são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da zona de firewall.
- **Configurações** contém as ações que o firewall aplica aos pacotes de tráfego.
- **Interfaces de rede/redes** são interfaces de rede e sub-redes adicionadas à zona de firewall.

Criar uma zona de firewall

É possível criar uma zona comum de firewall ou uma zona de firewall no dispositivo CPE.

Para criar uma zona de firewall:

1. Crie uma zona de firewall de uma das seguintes formas:
   - Para criar uma zona comum de firewall, vá para a seção **SD-WAN → Zonas de firewall** e, na parte superior da página, clique em **+ Zona de firewall**.
   - Para criar uma zona de firewall em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Zonas**, marque a caixa de seleção **Substituir** e clique em **+ Zona de firewall**.

   Uma tabela de zonas de firewall é exibida.
2. Na janela aberta, no campo **Nome**, insira o nome da zona de firewall. O comprimento máximo do nome é de 255 caracteres.

3. Na lista suspensa **Entrada**, selecione a ação que o firewall aplica a pacotes de tráfego de entrada:

   - **ACCEPT** para aceitar pacotes de tráfego. Essa é a configuração padrão.
   - **DROP** para descartar pacotes de tráfego.
   - **REJECT** para rejeitar pacotes de tráfego com uma mensagem `icmp-reject`.

4. Na lista suspensa **Saída**, selecione a ação que o firewall aplica a pacotes de tráfego de saída:

   - **ACCEPT** para aceitar pacotes de tráfego. Essa é a configuração padrão.
   - **DROP** para descartar pacotes de tráfego.
   - **REJECT** para rejeitar pacotes de tráfego com uma mensagem `icmp-reject`.

5. Na lista suspensa **Encaminhamento**, selecione a ação que o firewall aplica aos pacotes de tráfego encaminhados entre interfaces de rede e sub-redes:

   - **ACCEPT** para aceitar pacotes de tráfego. Essa é a configuração padrão.
   - **DROP** para descartar pacotes de tráfego.
   - **REJECT** para rejeitar pacotes de tráfego com uma mensagem `icmp-reject`.

6. Para ativar o mascaramento para substituir o endereço IP de origem dos pacotes de tráfego de saída da zona de firewall pelo endereço IP atribuído à interface de rede de saída:

   a. Marque a caixa de seleção **Mascaramento**. Esta caixa de seleção está desmarcada por padrão.

   b. Para substituir o endereço IP de origem apenas para pacotes de tráfego com a sub-rede de origem especificada, em **Sub-redes de origem de mascaramento**, clique em **+ Adicionar** e insira o prefixo IPv4 da sub-rede de origem.

      A sub-rede é especificada e exibida em **Sub-redes de origem de mascaramento**. É possível especificar diversas sub-redes ou excluir sub-redes. Para excluir uma sub-rede, clique no ícone de exclusão ✕ ao lado dela.

   c. Para substituir o endereço IP de destino apenas para pacotes de tráfego com a sub-rede de origem especificada, em **Sub-redes de destino de mascaramento**, clique em **+ Adicionar** e insira o prefixo IPv4 da sub-rede de destino.

      A sub-rede é especificada e exibida em **Sub-redes de destino de mascaramento**. É possível especificar diversas sub-redes ou excluir sub-redes. Para excluir uma sub-rede, clique no ícone de exclusão ✕ ao lado dela.

7. Desmarque a caixa de seleção **Limitar MSS a PMTU** caso não deseje que o firewall limite o Tamanho Máximo do Segmento (MSS) dos pacotes de tráfego retransmitidos através da zona do firewall ao valor da Unidade Máxima de Transmissão do Caminho (PMTU) menos 40. O objetivo de subtrair 40 é excluir o tamanho do cabeçalho TCP. Esta caixa de seleção é selecionada por padrão.

8. Caso deseje que o firewall mantenha um log dos pacotes de tráfego descartados na zona do firewall, marque a caixa de seleção **Registro de descartes**. Se os logs criados em um dispositivo CPE forem enviados para um servidor syslog, será possível visualizá-los no servidor syslog. Se os logs criados no dispositivo CPE forem armazenados localmente, será possível visualizá-los solicitando informações de diagnóstico. Esta caixa de seleção está desmarcada por padrão.

9. Se as interfaces de rede estiverem conectadas a switches ou roteadores L3 e você quiser retransmitir pacotes de tráfego de sub-redes desses switches ou roteadores L3, adicione uma sub-rede à zona de firewall. Para isso, em **Redes**, clique em **+ Adicionar** e insira um prefixo de sub-rede IPv4.

   A sub-rede é adicionada e exibida em **Redes**. É possível adicionar diversas sub-redes ou excluir sub-redes. Para excluir uma sub-rede, clique no ícone de exclusão ✕ ao lado dela.

10. Clique em **Criar**.

    A zona de firewall é criada e exibida na tabela.

11. Caso tenha criado uma zona de firewall em um dispositivo CPE, clique em **Salvar** na parte superior da área de configurações para salvar as configurações do dispositivo CPE.

É necessário adicionar interfaces de rede à zona de firewall criada. Faça isso ao criar ou editar uma interface de rede. Caso tenha criado uma zona de firewall em um dispositivo CPE, as interfaces de rede adicionadas à zona de firewall devem ser criadas no mesmo dispositivo CPE.

Clonar uma zona comum de firewall

É possível clonar a zona comum de firewall criada para criar uma zona comum de firewall idêntica com um nome diferente. Não é possível clonar zonas de firewall em um dispositivo CPE.

Para clonar uma zona comum de firewall:

1. No menu, acesse a seção **SD-WAN → Zonas de firewall**.

   Uma tabela de zonas de firewall comuns é exibida.

2. Clique na zona comum de firewall que deseja clonar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Clonar**.

4. Na janela aberta, insira um nome para a nova zona comum de firewall.

5. Clique em **Clonar**.

Um clone da zona comum de firewall com o novo nome é criado e exibido na tabela.

Visualizar o uso de uma zona comum de firewall

Se necessário, é possível verificar que modelos de firewall, modelos de CPE e dispositivos CPE estão usando a zona comum de firewall. Por exemplo, se uma zona comum de firewall estiver em uso, ela não pode ser excluída.

Para ver se uma zona comum de firewall está sendo usada:

1. No menu, acesse a seção **SD-WAN → Zonas de firewall**.

   Uma tabela de zonas de firewall comuns é exibida.

2. Clique na zona comum de firewall cujo uso deseja visualizar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Mostrar utilização**.

Isso abre uma janela com uma tabela de modelos de firewall, modelos de CPE e dispositivos CPE que estão usando a zona comum de firewall.

Editar uma zona de firewall

É possível editar uma zona comum de firewall ou uma zona de firewall no dispositivo CPE.

Editar uma zona comum de firewall

Ao editar uma zona comum de firewall, as novas configurações são aplicadas a todos os dispositivos CPE que usam a zona comum de firewall. Isso pode sobrecarregar o orquestrador se o número de dispositivos CPE for grande.

Para editar uma zona comum de firewall:

1. No menu, vá para a seção **SD-WAN → Zonas de firewall**.

   Uma tabela de zonas de firewall comuns é exibida.

2. Clique na zona comum de firewall que deseja editar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃.

3. Se necessário, edite as configurações da zona comum de firewall. Para obter uma descrição das configurações, consulte as instruções para criar uma zona de firewall.

4. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da zona comum de firewall.

   Isso abre uma janela de confirmação com o número de dispositivos CPE aos quais as novas configurações da zona comum de firewall serão aplicadas.

5. Clique em **Sim, alterar**.

A zona comum de firewall é modificada e atualizada na tabela.

Editar uma zona de firewall em um dispositivo CPE

Para editar uma zona de firewall em um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE no qual você deseja editar a zona de firewall.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Firewall** → **Zonas**.

   Uma tabela de zonas de firewall é exibida.

4. Marque a caixa de seleção **Substituir**.

5. Clique em **Editar** ao lado da zona de firewall que deseja editar.

6. Na janela aberta, se necessário, edite as configurações da zona de firewall. Para obter uma descrição das configurações, consulte as instruções para criar uma zona de firewall.

7. Clique em **Salvar**.

   A zona de firewall é modificada e atualizada na tabela.

8. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

Excluir uma zona de firewall

É possível excluir uma zona comum de firewall ou uma zona de firewall no dispositivo CPE.

As zonas de firewall excluídas não podem ser restauradas.

Excluir uma zona comum de firewall

Não é possível excluir uma zona comum de firewall se ela estiver sendo usada por pelo menos um modelo de firewall, modelo de CPE ou dispositivo CPE. Para excluir uma zona comum de firewall usada por modelos de firewall, modelos de CPE ou dispositivos CPE, primeiro remova a zona comum de firewall das configurações deles. É possível verificar que modelos de firewall, modelos de CPE e dispositivos CPE estão usando a zona comum de firewall.

Para excluir uma zona comum de firewall:

1. No menu, acesse a seção **SD-WAN** → **Zonas de firewall**.

   Uma tabela de zonas de firewall comuns é exibida.

2. Clique na zona comum de firewall que deseja excluir.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃.

3. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

A zona comum de firewall é excluída e não é mais exibida na tabela.

Excluir uma zona de firewall em um dispositivo CPE

Para excluir uma zona de firewall em um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE do qual deseja excluir a zona de firewall.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Selecione a guia **Firewall → Zonas**.

   Uma tabela de zonas de firewall é exibida.

4. Marque a caixa de seleção **Substituir**.

5. Clique em **Excluir** ao lado da zona de firewall que deseja excluir.

6. Na janela de confirmação, clique em **Excluir**.

   A zona de firewall é excluída e não é mais exibida na tabela.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

Gerenciar modelos de firewall

É possível visualizar a tabela de modelos de firewall na seção **SD-WAN →Modelos de firewall**. Por padrão, um **modelo de firewall padrão** é criado e se torna a base para todos os outros modelos de firewall criados. As informações sobre modelos de firewall são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do modelo de firewall.
- **Utilização** especifica se os dispositivos CPE usam o modelo de firewall:
  - **Sim**.
  - **Não**.
- **Proprietário** é o nome do usuário que criou o modelo de firewall.
- **Última atualização** é a data e hora em que as configurações do modelo de firewall foram modificadas pela última vez.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

É possível selecionar um modelo de firewall atribuído para ser pré-selecionado ao adicionar ou registrar manualmente um dispositivo CPE.

É possível gerenciar as configurações de modelos de firewall nas seguintes guias:

- **Configurações gerais** contém as configurações básicas do firewall.
- **Regras** contém as regras de firewall.
- **NAT** contém as configurações de conversão de endereços de rede. As seguintes guias são exibidas nesta guia:
  - **DNAT** contém as regras de DNAT.
  - **SNAT** contém as regras de SNAT.
- **Encaminhamento de zona** contém encaminhamentos entre zonas de firewall.
- **Conjuntos de endereços IP** contém conjuntos de IPs.

Criar um modelo de firewall

Para criar um modelo de firewall:

1. Vá para a seção **SD-WAN → Modelos de firewall**.
   Uma tabela de modelos de firewall é exibida.
2. Na parte superior da página, clique em **+ Modelo de firewall**.
3. Na janela aberta, insira o nome do modelo de firewall.
4. Clique em **Criar**.

   O modelo de firewall é criado e exibido na tabela.

É necessário configurar o modelo de firewall criado. Para obter detalhes sobre o gerenciamento de modelos de firewall, consulte Gerenciar modelos de firewall.

Selecionar um modelo de firewall atribuído

É possível selecionar um modelo de firewall atribuído para ser pré-selecionado ao adicionar ou registrar manualmente um dispositivo CPE.

Para selecionar um modelo de firewall atribuído:

1. Vá para a seção **SD-WAN → Modelos de firewall**.
   Uma tabela de modelos de firewall é exibida.

2. Clique no modelo de firewall que deseja tornar o modelo atribuído.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configurações gerais**, que exibe as principais configurações do modelo de firewall.

3. Na parte superior da área de configurações, em **Ações**, clique em **Definir como designado**.

O modelo de firewall se torna o modelo atribuído.

Importar um modelo de firewall

É possível exportar um modelo de firewall e depois importá-lo para outro modelo de firewall. As configurações do modelo de firewall são especificadas de acordo com as configurações do modelo de firewall importado. Durante a importação, selecione as guias que deseja deixar inalteradas. Um modelo de firewall para o qual outro modelo de firewall é importado permanece aplicado aos dispositivos CPE, mas as configurações desses dispositivos CPE não são modificadas.

Para importar um modelo de firewall:

1. Vá para a seção **SD-WAN → Modelos de firewall**.

   Uma tabela de modelos de firewall é exibida.

2. Clique no modelo de firewall que deseja exportar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configurações gerais**, que exibe as principais configurações do modelo de firewall.

3. Na parte superior da área de configurações, em **Ações**, clique em **Exportar**.

   Um arquivo comprimido no formato TAR.GZ é salvo no dispositivo local. O arquivo não contém informações sobre dispositivos CPE que usam o modelo de firewall.

4. Clique no modelo de firewall para o qual deseja importar outro modelo de firewall.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃⌃. Por padrão, é selecionada a guia **Configurações gerais**, que exibe as principais configurações do modelo de firewall.

5. Na parte superior da área de configurações, em **Ações**, clique em **Importar**.

6. Na janela aberta, desmarque as caixas de seleção ao lado das guias do modelo de firewall que deseja manter inalteradas após a importação.

7. No campo **Arquivo**, especifique o caminho para o arquivo TAR.GZ.

8. Clique em **Importar**.

As configurações do modelo de firewall são alteradas de acordo com as configurações do modelo de firewall importado.

Clonar um modelo de firewall

É possível clonar um modelo de firewall para criar um modelo idêntico com um nome diferente.

Para clonar um modelo de firewall:

1. Vá para a seção **SD-WAN → Modelos de firewall**.

   Uma tabela de modelos de firewall é exibida.

2. Clique no modelo de firewall que deseja clonar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃. Por padrão, é selecionada a guia **Configurações gerais**, que exibe as principais configurações do modelo de firewall.

3. Na parte superior da área de configurações, em **Ações**, clique em **Clonar**.

4. Na janela aberta, insira o nome do novo modelo de firewall.

5. Clique em **Clonar**.

Um clone do modelo de firewall com o novo nome é criado e exibido na tabela.

Visualizar o uso de um modelo de firewall

Se necessário, é possível verificar quais dispositivos CPE estão usando o modelo de firewall. Por exemplo, se um modelo de firewall estiver em uso, ele não pode ser excluído.

Para ver se um modelo de firewall está sendo usado:

1. Vá para a seção **SD-WAN → Modelos de firewall**.

   Uma tabela de modelos de firewall é exibida.

2. Clique no modelo de firewall cujas informações de uso deseja visualizar.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃. Por padrão, é selecionada a guia **Configurações gerais**, que exibe as principais configurações do modelo de firewall.

3. Na parte superior da área de configurações, em **Ações**, clique em **Mostrar CPEs associados**.

Isso abre uma janela com uma tabela de dispositivos CPE que estão usando o modelo de firewall.

Excluir um modelo de firewall

Não é possível excluir um modelo de firewall se ele estiver sendo usado por pelo menos um dispositivo CPE. Para excluir um modelo de firewall que está sendo usado por dispositivos CPE, primeiro altere o modelo de firewall dos dispositivos CPE. É possível verificar quais dispositivos CPE estão usando o modelo de firewall.

Os modelos de firewall excluídos não podem ser restaurados.

Para excluir um modelo de firewall:

1. Vá para a seção **SD-WAN → Modelos de firewall**.

   Uma tabela de modelos de firewall é exibida.

2. Selecione o modelo de firewall que deseja excluir.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⌃. Por padrão, é selecionada a guia **Configurações gerais**, que exibe as principais configurações do modelo de firewall.

3. Na parte superior da área de configurações, em **Ações**, clique em **Excluir**.

4. Na janela de confirmação, clique em **Excluir**.

O modelo de firewall é excluído e não é mais exibido na tabela.

Configurações básicas de firewall

É possível definir as configurações básicas de firewall em um modelo de firewall ou em um dispositivo CPE. As configurações básicas de firewall especificadas no modelo de firewall são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

O firewall aplica as ações especificadas em suas configurações básicas aos pacotes de tráfego. Os pacotes de tráfego são afetados se nenhuma regra de firewall tiver sido aplicada a eles e eles não tiverem sido encaminhados para nenhuma das zonas de firewall.

Para especificar as configurações básicas de firewall:

1. Especifique as configurações básicas de firewall de uma das seguintes formas:

   - Para editar as configurações básicas de firewall em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu e clique no modelo de firewall.

   - Para editar as configurações básicas de firewall em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall** e marque a caixa de seleção **Substituir**.

   Por padrão, é selecionada a guia **Configurações gerais**, que exibe as principais configurações do firewall.

2. Para desativar a proteção contra inundação SYN, desmarque a caixa de seleção **Proteção contra inundação syn**. Esta caixa de seleção é selecionada por padrão. Quando a proteção contra inundação SYN está ativada, um máximo de 25 pacotes de tráfego por segundo com os indicadores SYN, ACK, RST e FIN podem ser enviados para um dispositivo CPE.

3. Caso deseje que o firewall elimine pacotes de tráfego marcados como inválidos pela função conntrack, marque a caixa de seleção **Descartar pacotes inválidos**. Esta caixa de seleção está desmarcada por padrão.

4. Para desativar a tecnologia DPI (inspeção profunda de pacotes), desmarque a caixa de seleção **Ativar DPI**. Esta caixa de seleção é selecionada por padrão. A tecnologia DPI permite criar regras de firewall que se aplicam apenas a pacotes de tráfego do aplicativo especificado.

   Quando a tecnologia DPI está desativada, não é possível configurar a marcação de DPI, e as regras de firewall que usam a tecnologia DPI são automaticamente desativadas.

5. Na lista suspensa **Ação de ENTRADA padrão**, selecione a ação que o firewall aplica a pacotes de tráfego de entrada:

   - **ACCEPT** para aceitar pacotes de tráfego. Essa é a configuração padrão.
   - **DROP** para descartar pacotes de tráfego.
   - **REJECT** para rejeitar pacotes de tráfego com uma mensagem `icmp-reject`.

6. Na lista suspensa **Ação de SAÍDA padrão**, selecione a ação que o firewall aplica a pacotes de tráfego de saída:

   - **ACCEPT** para aceitar pacotes de tráfego. Essa é a configuração padrão.
   - **DROP** para descartar pacotes de tráfego.
   - **REJECT** para rejeitar pacotes de tráfego com uma mensagem `icmp-reject`.

7. Na lista suspensa **Ação de ENCAMINHAMENTO padrão**, selecione a ação que o firewall aplica aos pacotes de tráfego encaminhados entre interfaces de rede e sub-redes:

   - **ACCEPT** para aceitar pacotes de tráfego. Essa é a configuração padrão.
   - **DROP** para descartar pacotes de tráfego.
   - **REJECT** para rejeitar pacotes de tráfego com uma mensagem `icmp-reject`.

8. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Configurar a marcação de DPI

O Kaspersky SD-WAN é compatível com a criação de regras de firewall aplicadas apenas a pacotes de tráfego do aplicativo especificado. É possível especificar as marcas de DPI que determinam os pacotes de tráfego aos quais a regra é aplicada. Não é possível configurar a marcação de DPI se a tecnologia de marcação de DPI tiver sido desativada nas configurações básicas do firewall.

É possível configurar a marcação de DPI em um modelo de firewall ou em um dispositivo CPE. As configurações de marcação de DPI especificadas no modelo de firewall são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para configurar a marcação de DPI:

1. Configure a marcação de DPI para o firewall de uma das seguintes formas:

   - Para configurar a marcação de DPI em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Marcação de DPI**.
   - Para configurar a marcação de DPI em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Marcação de DPI** e marque a caixa de seleção **Substituir**.

   As configurações de marcação de DPI são exibidas.

2. Marque as caixas de seleção ao lado das marcas de DPI que devem controlar quais regras de firewall se aplicam a quais pacotes de tráfego.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Gerenciar regras de firewall

Para visualizar a tabela de regras de firewall em um modelo de firewall ou em um dispositivo CPE:

- Para visualizar a tabela de regras de firewall em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras**.

- Para visualizar a tabela de regras de firewall em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Firewall → Regras**.

As seguintes regras de firewall são criadas por padrão:

- **Allow-GENEVE** permite que o dispositivo CPE receba pacotes GENEVE da zona de firewall WAN. Os pacotes GENEVE são tráfego Kaspersky SD-WAN encapsulado.

- **Allow-DHCP-Renew** permite que o dispositivo CPE receba pacotes BOOTP da zona de firewall WAN, o que é necessário para o funcionamento do DHCP.

- **Allow-IGMP** permite que o dispositivo CPE receba pacotes IGMP da zona de firewall WAN, o que é necessário para o funcionamento do VRRP e do multicast.

- As seguintes regras de firewall são temporariamente desativadas até que o suporte total para IPv6 esteja disponível no Kaspersky SD-WAN:

  - **Allow-DHCPv6** permite que o dispositivo CPE receba pacotes DHCPv6 da zona de firewall WAN, o que é necessário para o funcionamento do IPv6.

  - **Allow-MLD** permite que o dispositivo CPE receba pacotes MLD da zona de firewall WAN, o que é necessário para o funcionamento do IPv6.

  - **Allow-ICMPv6-Input** permite que o dispositivo CPE receba pacotes ICMPv6 da zona de firewall WAN, o que é necessário para o funcionamento do IPv6.

  - **Allow-ICMPv6-Forward-From-Wan** permite que o dispositivo CPE receba pacotes ICMPv6 da zona de firewall WAN. Esses pacotes são encaminhados para a zona de firewall LAN, o que é necessário para o funcionamento do IPv6.

  - **Allow-ICMPv6-Forward-From-Lan** permite que o dispositivo CPE receba pacotes ICMPv6 da zona de firewall LAN. Esses pacotes são encaminhados para a zona de firewall WAN, o que é necessário para o funcionamento do IPv6.

- **Explicit-deny-http-on-wan** bloqueia o recebimento de pacotes de tráfego TCP pelo dispositivo CPE com a porta de destino 80 para impedir o acesso da zona de firewall WAN ao servidor Web do dispositivo CPE.

- **Explicit-deny-https-on-wan** bloqueia o recebimento de pacotes de tráfego TCP pelo dispositivo CPE com a porta de destino 443 para impedir o acesso da zona de firewall WAN ao servidor Web do dispositivo CPE.

Para que as regras de firewall padrão funcionem corretamente, adicione interfaces de rede **sd-wan<0–4>** à zona de firewall WAN. É possível adicionar interfaces de rede a uma zona de firewall ao criar ou editar uma interface de rede.

As informações sobre as regras de firewall são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da regra de firewall.
- **Detalhes** contém critérios segundo os quais o firewall aplica a regra aos pacotes de tráfego.
- **Ação** é a ação que a regra de firewall aplica aos pacotes de tráfego.

Criar uma regra de firewall

É possível criar uma regra de firewall em um modelo de firewall ou em um dispositivo CPE. Regras de firewall criadas em um modelo de firewall são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma regra de firewall:

1. Crie uma regra de firewall de uma das seguintes formas:
   - Para criar uma regra de firewall em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras**.
   - Para criar uma regra de firewall em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Regras** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de firewall é exibida.
2. Clique em **+ Regra**.
3. Na janela aberta, no campo **Nome**, insira o nome da regra de firewall. O comprimento máximo do nome é de 255 caracteres.
4. Na lista suspensa **Ação**, selecione a ação que a regra de firewall aplica a pacotes de tráfego:
   - **ACCEPT** para aceitar pacotes de tráfego. Essa é a configuração padrão.
   - **DROP** para descartar pacotes de tráfego.
   - **REJECT** para rejeitar pacotes de tráfego com uma mensagem `icmp-reject`.
   - **ADJ-MSS** para alterar o valor no campo MSS no cabeçalho TCP dos pacotes de tráfego para o valor de MSS especificado. Ao selecionar esse valor, no campo **Valor de MSS**, insira o valor de MSS. Intervalo de valores: 68 a 10.000.

5. Especifique os critérios segundo os quais o firewall deve aplicar a regra de firewall aos pacotes de tráfego:

   a. Para aplicar a regra de firewall apenas a pacotes de tráfego com os endereços IP ou sub-redes de origem ou destino especificados, na lista suspensa **Conjunto de endereços IP**, selecione um conjunto de IPs criado. Ao selecionar um valor nessa lista suspensa, os blocos **IP de origem** e **IP de destino** ficam indisponíveis.

   b. Para aplicar a regra de firewall apenas a pacotes de tráfego com a versão dos endereços IPv4 ou sub-redes de origem ou destino, na lista suspensa **Versão de IP**, selecione **IPv4**: caso nenhum valor seja selecionado, a regra de firewall é aplicada a pacotes de tráfego com qualquer versão de endereços IP ou sub-redes de origem ou destino.

   c. Para aplicar a regra de firewall apenas a pacotes de tráfego com a zona de firewall de origem especificada, na lista suspensa **Zona de origem**, selecione a zona de firewall criada.

   d. Para aplicar a regra de firewall apenas a pacotes de tráfego com a zona de firewall de destino especificada, na lista suspensa **Zona de destino**, selecione uma zona de firewall criada.

   e. Para aplicar a regra de firewall apenas a pacotes de tráfego com o endereço ou prefixo IPv4 de origem especificado, em **IP de origem**, clique em **+ Adicionar** e insira o endereço ou prefixo IPv4 de origem.

      O endereço ou prefixo IPv4 é especificado e exibido em **IP de origem**. É possível especificar vários endereços ou prefixos IPv4 ou excluir endereços ou prefixos IPv4. Para excluir um endereço ou prefixo IPv4, clique no ícone de exclusão ✕ ao lado dele.

   f. Para aplicar a regra de firewall apenas a pacotes de tráfego com o endereço ou prefixo IPv4 de destino especificado, em **IP de destino**, clique em **+ Adicionar** e insira o endereço ou prefixo IPv4 de destino.

      O endereço ou prefixo IPv4 é especificado e exibido em **IP de destino**. É possível especificar vários endereços ou prefixos IPv4 ou excluir endereços ou prefixos IPv4. Para excluir um endereço ou prefixo IPv4, clique no ícone de exclusão ✕ ao lado dele.

   g. Para aplicar a regra de firewall apenas a pacotes de tráfego do protocolo especificado, selecione um protocolo na lista suspensa **Protocolo**. Ao selecionar uma opção nessa lista suspensa, a lista suspensa **Protocolo de DPI** fica indisponível.

      Com **TCP** ou **UDP** selecionado, para aplicar a regra de firewall apenas a pacotes de tráfego com as portas de origem e/ou destino especificadas:

      1. No campo **Porta de origem**, insira um número de porta de origem ou um intervalo de números de porta de origem.

      2. No campo **Porta de destino**, insira um número de porta de destino ou um intervalo de números de porta de destino.

      Intervalo de valores: 0 a 65.535. O formato do intervalo de números de porta é `<primeiro valor>-<último valor>`. Por exemplo, `10` ou `10-15`.

   h. Para aplicar a regra de firewall apenas a pacotes de tráfego do aplicativo especificado, selecione um aplicativo na lista suspensa **Protocolo de DPI**.

      O tráfego é atribuído a aplicativos que usam a tecnologia DPI, que coloca uma carga adicional na CPU do dispositivo CPE.

      É possível especificar as marcas de DPI que determinam os pacotes de tráfego aos quais a regra é aplicada. Caso tenha desativado a tecnologia DPI ao especificar as configurações básicas do firewall, a regra de firewall será automaticamente desativada.

6. Clique em **Criar**.

   A regra de firewall é criada e exibida na tabela.

7. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Por padrão, a regra de firewall está desativada. É necessário ativar a regra de firewall para que ela seja aplicada aos pacotes de tráfego.

Configurar a ordem das regras de firewall

As regras de firewall são aplicadas aos pacotes de tráfego em ordem decrescente, começando com a primeira regra de firewall no topo da tabela. Por padrão, as regras de firewall são exibidas na tabela na ordem de criação. Regras de firewall criadas há mais tempo são exibidas mais acima na tabela.

É possível configurar a ordem em que as regras de firewall são aplicadas em um modelo de firewall ou em um dispositivo CPE. A ordem em que as regras de firewall são aplicadas, especificada no modelo de firewall, é propagada automaticamente para todos os dispositivos CPE que usam o modelo.

Para configurar a ordem em que as regras de firewall são aplicadas:

1. Edite a ordem em que as regras de firewall são aplicadas de uma das seguintes formas:

   - Para configurar a ordem em que as regras de firewall são aplicadas em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras**.

   - Para configurar a ordem em que as regras de firewall são aplicadas em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Regras** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de firewall é exibida.

2. Configure a ordem em que as regras de firewall são aplicadas clicando nos botões **Para cima** e **Para baixo** ao lado delas.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Ativar ou desativar uma regra de firewall

Por padrão, as regras de firewall são criadas no estado desativado. É necessário ativar a regra de firewall para que ela seja aplicada aos pacotes de tráfego.

É possível ativar ou desativar uma regra de firewall em um modelo de firewall ou em um dispositivo CPE. Uma regra de firewall ativada ou desativada em um modelo de firewall é ativada ou desativada automaticamente em todos os dispositivos CPE que usam o modelo.

Para ativar ou desativar uma regra de firewall:

1. Ative ou desative uma regra de firewall de uma das seguintes formas:

   - Para ativar ou desativar uma regra de firewall em um modelo de firewall, vá para a seção **SD-WAN** → **Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras**.

   - Para ativar ou desativar uma regra de firewall em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall** → **Regras** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de firewall é exibida.

2. Clique em **Ativar** ou **Desativar** ao lado da regra de firewall que deseja ativar ou desativar.

   A regra de firewall é ativada ou desativada.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Editar uma regra de firewall

É possível editar uma regra de firewall em um modelo de firewall ou em um dispositivo CPE. Uma regra de firewall modificada em um modelo de firewall é modificada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma regra de firewall:

1. Edite uma regra de firewall de uma das seguintes formas:

   - Para editar uma regra de firewall em um modelo de firewall, vá para a seção **SD-WAN** → **Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras**.

   - Para editar uma regra de firewall em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall** → **Regras** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de firewall é exibida.

2. Clique em **Editar** ao lado da regra de firewall que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da regra de firewall. Para obter uma descrição das configurações, consulte as instruções para criar uma regra de firewall.

4. Clique em **Salvar**.

   A regra de firewall é modificada e atualizada na tabela.

5. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Excluir uma regra de firewall

É possível excluir uma regra de firewall em um modelo de firewall ou em um dispositivo CPE. Uma regra de firewall excluída de um modelo de firewall é excluída automaticamente de todos os dispositivos CPE que usam o modelo.

As regras de firewall excluídas não podem ser restauradas.

Para excluir uma regra de firewall:

1. Exclua uma regra de firewall de uma das seguintes formas:

   - Para excluir uma regra de firewall em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras**.
   - Para excluir uma regra de firewall em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Regras** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de firewall é exibida.

2. Clique em **Excluir** ao lado da regra de firewall que deseja excluir.

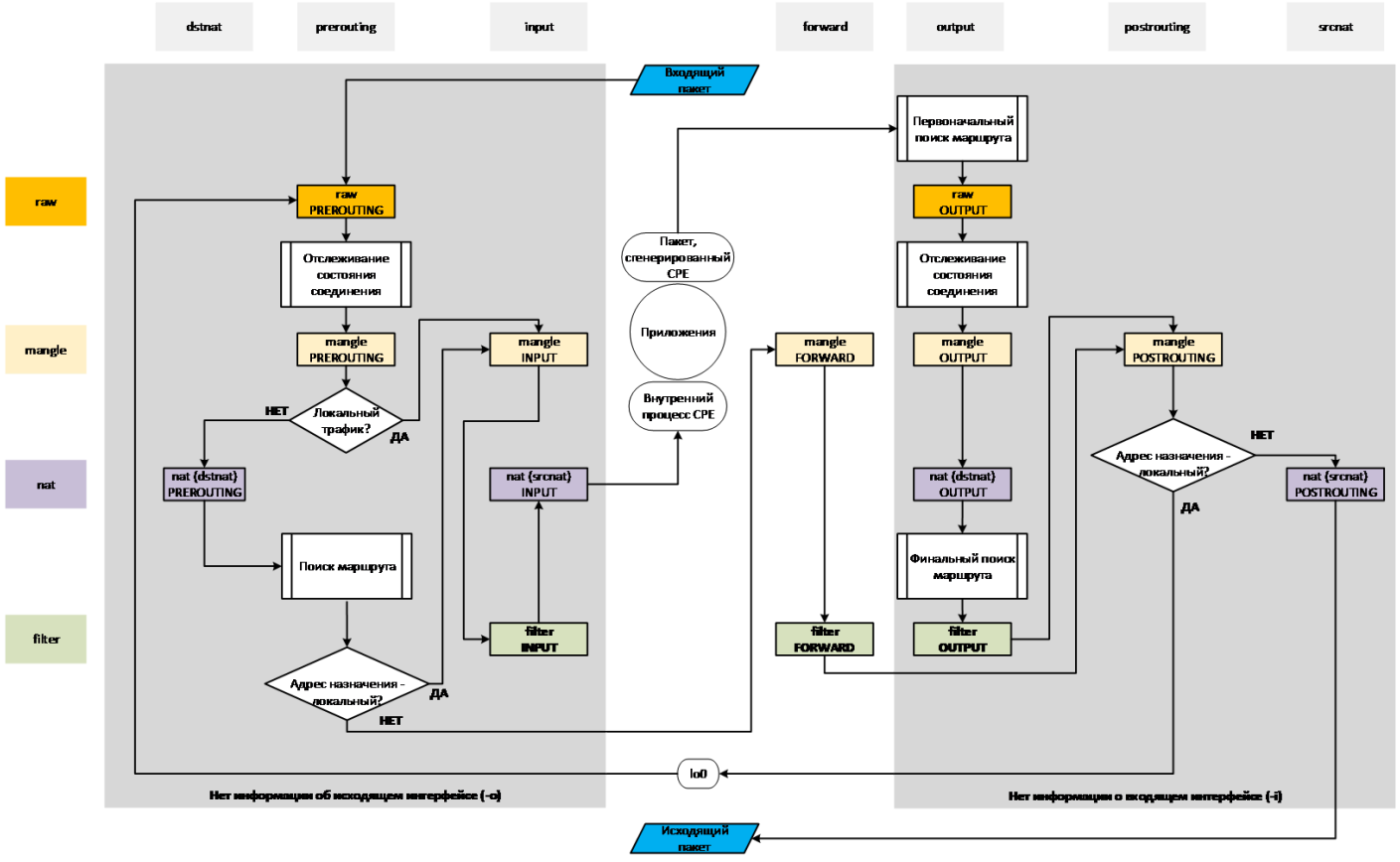
3. Na janela de confirmação, clique em **Excluir**.

   A regra de firewall é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Gerenciar regras avançadas de firewall

As regras avançadas implementam o modelo de filtro de pacotes clássico no estilo iptables. A figura abaixo mostra o diagrama de processamento de pacotes com regras avançadas:



Esquema de processamento de pacotes com regras avançadas que seguem o modelo de filtro de pacotes clássico no estilo iptables

Para visualizar a tabela de regras avançadas de firewall em um modelo de firewall ou em um dispositivo CPE:

- Para visualizar a tabela de regras avançadas de firewall em um modelo de firewall, acesse a seção **SD-WAN** → **Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras avançadas**.
- Para visualizar a tabela de regras avançadas de firewall em um dispositivo CPE, acesse a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **Firewall** → **Regras avançadas**.

Critérios de correspondência adicionais para regras avançadas

Nas regras avançadas de firewall, use critérios de correspondência adicionais para selecionar pacotes. Esta seção descreve esses critérios e seus parâmetros.

Pacote fragmentado

Este critério é atendido quando fragmentos de pacotes IP são detectados no tráfego, mas não para o primeiro fragmento. Esses pacotes são marcados provisoriamente com uma marca especial, portanto, esse critério não pode ser usado simultaneamente com o critério **Corresponder por marca**. Ativar a configuração **Pacote fragmentado** desativa automaticamente a configuração **Corresponder por marca**, se estiver ativada, e a bloqueia.

Corresponder por marca

Este critério é atendido quando um campo com uma marca definida anteriormente usando a ação `MARK` é detectado.

Parâmetros:

Valor

Marque o valor no formato hexadecimal (`0x0–0xFFFFFFFF`) ou decimal (`0–4294967295`).

Exemplos: `0x1`; `1`

Máscara

Valor de máscara de bits opcional no formato hexadecimal (`0x0–0xFFFFFFFF`) ou decimal (`0–4294967295`). Se especificado, é aplicado com um AND bit a bit à marca para especificar bits individuais que devem corresponder.

Exemplo: `0xFF`

TOS

Esse critério é atendido quando o valor especificado do campo `TOS` (`Tipo de serviço`) é detectado no cabeçalho IPv4 de um pacote.

Parâmetros:

Valor

Valor TOS no formato hexadecimal (`0x0–0xFF`) ou decimal (`0–255`).

Máscara

Valor de máscara de bits opcional no formato hexadecimal (`0x0–0xFF`) ou decimal (`0–255`). Se especificado, é aplicado com um AND bit a bit ao `TOS` para especificar bits individuais que devem corresponder ao valor definido.

Corresponder por string

O critério é atendido quando os caracteres especificados são encontrados no pacote em texto ou notação hexadecimal.

Parâmetros:

Buscar padrão

Um padrão de pesquisa em texto ou notação hexadecimal. O comprimento máximo é de 255 caracteres. Os seguintes caracteres são compatíveis:

- Letras maiúsculas (A–Z)
- Letras minúsculas (a–z)
- Algarismos (0–9)
- Caracteres especiais (_ - . , : ; / + = @ ( ) ! ?)
- O caractere de espaço

Algoritmo

Algoritmo de comparação de strings para pesquisa:

- BM (Boyer–Moore)
- KMP (Knuth–Morris–Pratt).

Intervalo de posições

Intervalo de bytes no pacote pesquisado em busca de strings correspondentes. Os índices de byte são baseados em zero. Se não for especificado, o tamanho do pacote é usado.

String HEX

Se ativado, o valor no campo **Padrão de pesquisa** é tratado como uma string hexadecimal.

Ignorar maiúscula ou minúscula

Se ativado, maiúsculas e minúsculas são ignoradas.

Corresponder por recente

Este critério é aplicado com base na atividade anterior dos links. Se ativado, permite criar dinamicamente uma lista de endereços IP e, em seguida, procurar pacotes nessa lista.

Parâmetros:

Nome da lista

Nome da lista para a pesquisa.

Ação

Ação a ser executada com a lista:

- `set` (adicionar um endereço IP à lista)
- `rcheck` (procurar um endereço IP na lista sem atualizar a hora)
- `update` (procurar um endereço IP e atualizar a hora)
- `update` (procurar um endereço IP na lista e atualizar a hora)
- `remove` (remover um endereço IP da lista)

Flags TCP inválidas

Este critério é atendido quando uma combinação inválida de flags TCP (comumente usadas em técnicas de verificação de sub-rede) é detectada em um pacote.

Quando esta configuração é ativada, o valor do campo **Protocolo** na seção **Geral** é automaticamente definido como `TCP`.

Configurações:

Combinações de flags

Permite selecionar combinações de flags correspondentes a técnicas de verificação amplamente utilizadas:

- Todas as flags (verificação TCP ALL)
- Flags vazias (verificação TCP NULL)
- Flags FIN+ACK (verificação Maimon)
- Flag ACK em uma sessão não estabelecida (verificação TCP ACK)
- Flags FIN+PSH+URG (verificação Xmas)

Limite da taxa

Este critério é atendido se o valor de pacotes por segundo não exceder o limite configurado com base no algoritmo "token bucket".

Parâmetros:

Limite, pacotes/s

Especifica a taxa máxima permitida em pacotes por segundo. Uma regra com o limite especificado é acionada somente no tráfego cuja taxa não exceda o limite, levando em consideração o pico (veja abaixo). Os pacotes cuja taxa excede o limite não são processados por esta regra.

Rajada, pacotes

O número máximo de pacotes que podem passar de uma só vez além do limite definido. Quando esgotado, é reabastecido a uma taxa constante igual ao valor no campo **Limite, pacotes/s**.

Acionar no TCP SYN

Critérios adicionais para a correspondência de pacotes TCP que contenham a flag `SYN`. Quando esta configuração é ativada, o valor do campo **Protocolo** na seção **Geral** é automaticamente definido como `TCP`.

Código para dispositivos móveis

Esse critério é atendido quando um código móvel é detectado no tráfego HTTP não criptografado. Requer DPI ativado para detectar o tráfego HTTP, inclusive em portas não padrão.

Ativar esta opção desativa automaticamente todas as outras opções de correspondência avançada (configurações **Protocolo** e **DPI** na seção **Principal**) e todos os outros critérios avançados na seção **Correspondências adicionais**.

Parâmetros:

Tipos de código para dispositivos móveis

Permite selecionar um ou mais tipos de código móvel que devem acionar o critério.

- Applets Java
- Montagens WebAsm
- Scripts JavaScript/ECMAScript
- JavaScript no corpo da página
- Controles ActiveX
- Scripts/documentos PDF
- Scripts/documentos PostScript
- Animações/scripts Adobe Flash
- Scripts VB/VBA

Correspondência por comandos de protocolo da camada de aplicativo

O critério é acionado quando os comandos especificados de determinados protocolos da camada de aplicativo são detectados no tráfego não criptografado. Para usar esse critério, você precisa ativar a função DPI nas configurações básicas do firewall.

Você pode especificar os seguintes protocolos da camada de aplicativo e seus comandos:

Protocolo	Comando
HTTP	GET POST PUT DELETE HEAD OPTIONS CONNECT
SMTP	HELO MAIL RCPT DATA QUIT RSET VRFY NOOP
SIP	INVITE ACK BYE REGISTER OPTIONS
IMAP	STARTTLS AUTHENTICATE LOGIN SELECT EXAMINE CREATE DELETE RENAME SUBSCRIBE UNSUBSCRIBE LIST LSUB STATUS APPEND CHECK EXPUNGE SEARCH FETCH COPY
POP3	USER PASS STAT LISTA RETR EXC NOOP RSET TOP UIDL

FTP control	USER PASS QUIT LISTA RETR STOR DELE RMD REMOVE DIRECTORY MKD MAKE DIRECTORY PASV EPSV

Você pode usar esse critério ao criar ou editar regras de firewall avançadas. Para fazer isso, na seção **Geral** da área de configurações avançadas da regra, ative o botão de alternância **DPI**, selecione um protocolo da camada de aplicativo na lista suspensa **Protocolo específico** e selecione um comando na lista suspensa **Comando**. Se você selecionar "Qualquer", o critério será acionado por qualquer um dos comandos listados no protocolo selecionado.

Criar uma regra avançada

É possível criar uma regra avançada em um modelo de firewall ou em um dispositivo CPE. Uma regra avançada criada em um modelo de firewall é criada automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma regra avançada:

1. Crie uma regra avançada de uma das seguintes formas:

   - Para criar uma regra avançada em um modelo de firewall, acesse a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras avançadas**.
   - Para criar uma regra de firewall em um dispositivo CPE, acesse a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Regras avançadas** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras avançadas de firewall é exibida.

2. Clique em **+Adicionar**.

   A janela de criação de regra avançada é aberta.

3. Especifique as configurações básicas na seção **Geral**.

   a. Insira o nome da regra avançada no campo **Nome**. O comprimento máximo do nome é de 255 caracteres. Caracteres válidos: A-Z, a-z, 0-9, _ - . , : ; / + = @ ( ) ! ? e espaços.

   b. Se necessário, insira uma descrição para a regra avançada no campo **Descrição**.

   c. Se necessário, especifique uma ou mais tags de política selecionando-as na lista suspensa **Tags de política**. Uma regra marcada se torna inativa por padrão. É possível ativá-la mais tarde.

   Usando tags de política, é possível ativar ou desativar simultaneamente um conjunto de regras que atendem a uma determinada finalidade. Também é possível integrar um sistema de proteção de dados externo e ativar ou desativar tags de política por meio da API.

d. Especifique a tabela de firewall à qual você deseja adicionar a regra avançada selecionando-a na lista suspensa **Tabela**. As seguintes tabelas estão disponíveis:

- FILTRAR
- DESTRINCHAR
- NAT
- BRUTO

e. Para a tabela selecionada, especifique a cadeia à qual você deseja adicionar a regra avançada selecionando-a na lista suspensa **Cadeia**. O conjunto de cadeias disponíveis depende da tabela selecionada na etapa anterior:

- FILTRAR
  - ENTRADA
  - ENCAMINHAMENTO
  - SAÍDA
- DESTRINCHAR
  - ENTRADA
  - ENCAMINHAMENTO
  - SAÍDA
  - PRÉ-ROTEAMENTO
  - PÓS-ROTEAMENTO
- NAT
  - PRÉ-ROTEAMENTO
  - PÓS-ROTEAMENTO
  - ENTRADA
  - SAÍDA
- BRUTO
  - SAÍDA
  - PRÉ-ROTEAMENTO

f. Se necessário, especifique o protocolo ao qual você deseja aplicar a regra avançada selecionando-o na lista suspensa **Protocolo**:

- TCP
- UDP
- ICMP
- Todos (a regra se aplica a todos os protocolos acima)

Se você selecionou o protocolo ICMP, especifique o tipo e o código do pacote ICMP no qual deseja que a regra seja acionada. Para fazer isso, nos campos **Tipo** e **Código**, insira um valor de `0` a `255`.

g. Configure a correspondência de DPI conforme necessário:

1. Ative o botão de alternância **DPI**.
2. Especifique o protocolo do aplicativo ou o ID do serviço/aplicativo no qual você deseja que a regra seja acionada selecionando-o na lista **Protocolos específicos**.
3. Se necessário, configure a correspondência com base nos comandos dos protocolos da camada do aplicativo se você tiver selecionado um dos seguintes protocolos como o critério de correspondência de DPI: `HTTP`, `SMTP`, `SIP`, `IMAP`, `POP3`, `FTP control`.

> Não é possível usar a correspondência de **DPI** simultaneamente com a correspondência de **Protocolo** da etapa anterior. Ao usar a correspondência de **DPI**, a configuração **Protocolo** é bloqueada e os valores especificados para ela são ignorados.

h. Em **Posicionamento da regra**, configure a ordem em que a regra avançada é adicionada à lista de regras avançadas:

1. Especifique o tipo de posicionamento da regra avançada:
   - As pré-regras são inseridas antes de outras regras.
   - As pós-regras são anexadas ao final da tabela após outras regras.
2. Especifique o posicionamento da regra avançada na tabela:
   - Início da tabela
   - Fim da tabela
   - Após a regra avançada especificada

i. Se necessário, especifique o endereço IP de origem e o endereço IP de destino nos quais você deseja que a regra seja acionada.

Se você quiser que a regra seja acionada em todos os endereços IP de origem ou destino, exceto para os endereços especificados, marque a caixa de seleção **Fazer uma exclusão** para o campo correspondente.

j. Se necessário, especifique as interfaces de origem ou destino usando os campos em **Interfaces**.

k. Especifique a ação de destino que você deseja que a regra avançada aplique ao pacote quando acionada; para fazer isso, selecione um valor na lista suspensa **Destino**:

- ACEITAR
- DESCARTAR
- TTL
- REJEITAR
- MARCAR
- TOS
- LOG
- VOLTAR
- DNAT
- CLASSIFICAR

A escolha das ações depende da tabela selecionada. Ao selecionar as ações TTL, MARK, TOS, DNAT, CLASSIFY, você também precisa especificar valores adicionais que devem ser adicionados ao pacote.

4. Configure critérios de correspondência adicionais para a regra avançada na seção **Correspondências adicionais**. Para obter uma descrição detalhada das configurações de critérios, consulte a seção Critérios de correspondência adicionais para regras avançadas na Ajuda.

5. Se necessário, visualize o comando iptables resultante que será executado no dispositivo CPE após a regra ser aplicada clicando em **Exibir comando** na parte superior da área de configuração.

6. Clique em **Criar**.

   A regra avançada é criada e exibida na tabela.

7. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Ativar e desativar regras avançadas

É possível ativar ou desativar uma regra avançada de firewall em um modelo de firewall ou em um dispositivo CPE. Uma regra avançada de firewall ativada ou desativada em um modelo de firewall é ativada ou desativada automaticamente em todos os dispositivos CPE que usam o modelo.

Para ativar ou desativar uma regra avançada:

1. Ative ou desative a regra avançada de uma das seguintes formas:

   - Para ativar ou desativar uma regra avançada em um modelo de firewall, acesse a seção **SD-WAN** → **Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras avançadas**.

   - Para ativar ou desativar uma regra avançada em um dispositivo CPE, acesse a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **Regras avançadas** e ative o botão de alternância **Substituir**.

   A tabela de regras avançadas é exibida.

2. Defina o botão de alternância como **Desativado** ou **Ativado** para desativar ou ativar as regras avançadas conforme necessário.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Editar uma regra avançada

É possível editar uma regra avançada em um modelo de firewall ou em um dispositivo CPE. Uma regra avançada modificada em um modelo de firewall é modificada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma regra avançada:

1. Edite uma regra avançada de uma das seguintes formas:

   - Para editar uma regra avançada em um modelo de firewall, acesse a seção **SD-WAN** → **Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras avançadas**.

   - Para editar uma regra avançada em um dispositivo CPE, acesse a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall** → **Regras avançadas** e marque a caixa de seleção **Substituir**.

   A tabela de regras avançadas é exibida.

2. Selecione a regra avançada que deseja editar na tabela e clique no botão **Editar**.

3. Uma janela é aberta para editar as configurações da regra avançada conforme necessário. Para obter uma descrição das configurações, consulte as instruções para criar uma regra avançada.

4. Clique em **Salvar**.

   A regra avançada é modificada e atualizada na tabela.

5. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Excluir uma regra avançada

É possível excluir uma regra avançada em um modelo de firewall ou em um dispositivo CPE. Uma regra avançada excluída em um modelo de firewall é modificada automaticamente em todos os dispositivos CPE que usam o modelo.

As regras avançadas excluídas não podem ser restauradas.

Para excluir uma regra avançada:

1. Exclua uma regra avançada de uma das seguintes formas:

   - Para excluir uma regra avançada em um modelo de firewall, acesse a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Regras avançadas**.
   - Para excluir uma regra avançada em um dispositivo CPE, acesse a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Regras avançadas** e ative o botão de alternância **Substituir**.

   A tabela de regras avançadas é exibida.

2. Selecione uma ou mais regras avançadas que deseja excluir na tabela e clique no botão **Excluir**.
3. Confirme a exclusão clicando no botão **Excluir** na janela exibida.

   As regras avançadas são excluídas e não são mais exibidas na tabela.

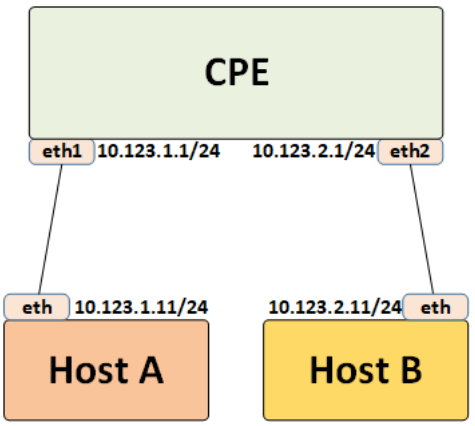
4. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Cenário: ocultar um dispositivo CPE no caminho de tráfego usando regras avançadas de firewall

Ao implementar um dispositivo CPE em um site remoto, os administradores geralmente não controlam totalmente as ações dos usuários na rede interna onde o dispositivo está localizado. Em tal situação, pode ser necessário excluir a possibilidade de o dispositivo CPE ser detectado como um nó ativo na rede ao verificar de dentro da rede interna. Você pode ocultar o dispositivo CPE na topologia de rede usando regras avançadas de firewall.

Este cenário descreve as etapas para criar regras avançadas que ocultam o dispositivo CPE da detecção por ferramentas padrão de verificação de rede.

Estado inicial



Topologia da rede

O estado inicial dos componentes da rede é o seguinte:

- Dois hosts, A e B, estão conectados ao dispositivo CPE.
- As interfaces `eth1` e `eth2` no CPE estão na mesma zona.
- Os firewalls nos hosts A e B estão configurados para permitir o tráfego ICMP.
- O host A rastreia a rota para o host B usando `traceroute`:

  ```
  tracert -d 10.123.2.11
  ```

  Resultado:

  ```
  1 10.123.1.1
  2 10.123.2.11
  ```

  Interpretação do resultado:

  O rastreamento revela um nó intermediário entre os hosts, que é o dispositivo CPE.

- A análise do tráfego de rede no dispositivo CPE para o protocolo ICMP entre os hosts A e B usando o comando `tcpdump -i any net 10.123.0.0/16` mostra o seguinte:

```
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 102, length 72
eth1 Out ARP, Request who-has 10.123.1.11 tell 10.123.1.1, length 28
eth1 In ARP, Reply 10.123.1.11 is-at bc:24:11:0a:91:06 (oui Unknown), length 28
eth1 Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit, length 100
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 103, length 72
eth1 Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit, length 100
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 104, length 72
eth1 Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit, length 100
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 105, length 72
eth2 Out ARP, Request who-has 10.123.2.11 tell 10.123.2.1, length 28
eth2 In ARP, Reply 10.123.2.11 is-at bc:24:11:59:58:b7 (oui Unknown), length 28
eth2 Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 105, length 72
eth2 In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 105, length 72
eth1 Out IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 105, length 72
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 106, length 72
eth2 Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 106, length 72
eth2 In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 106, length 72
eth1 Out IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 106, length 72
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 107, length 72
eth2 Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 107, length 72
eth2 In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 107, length 72
eth1 Out IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 107, length 72
```

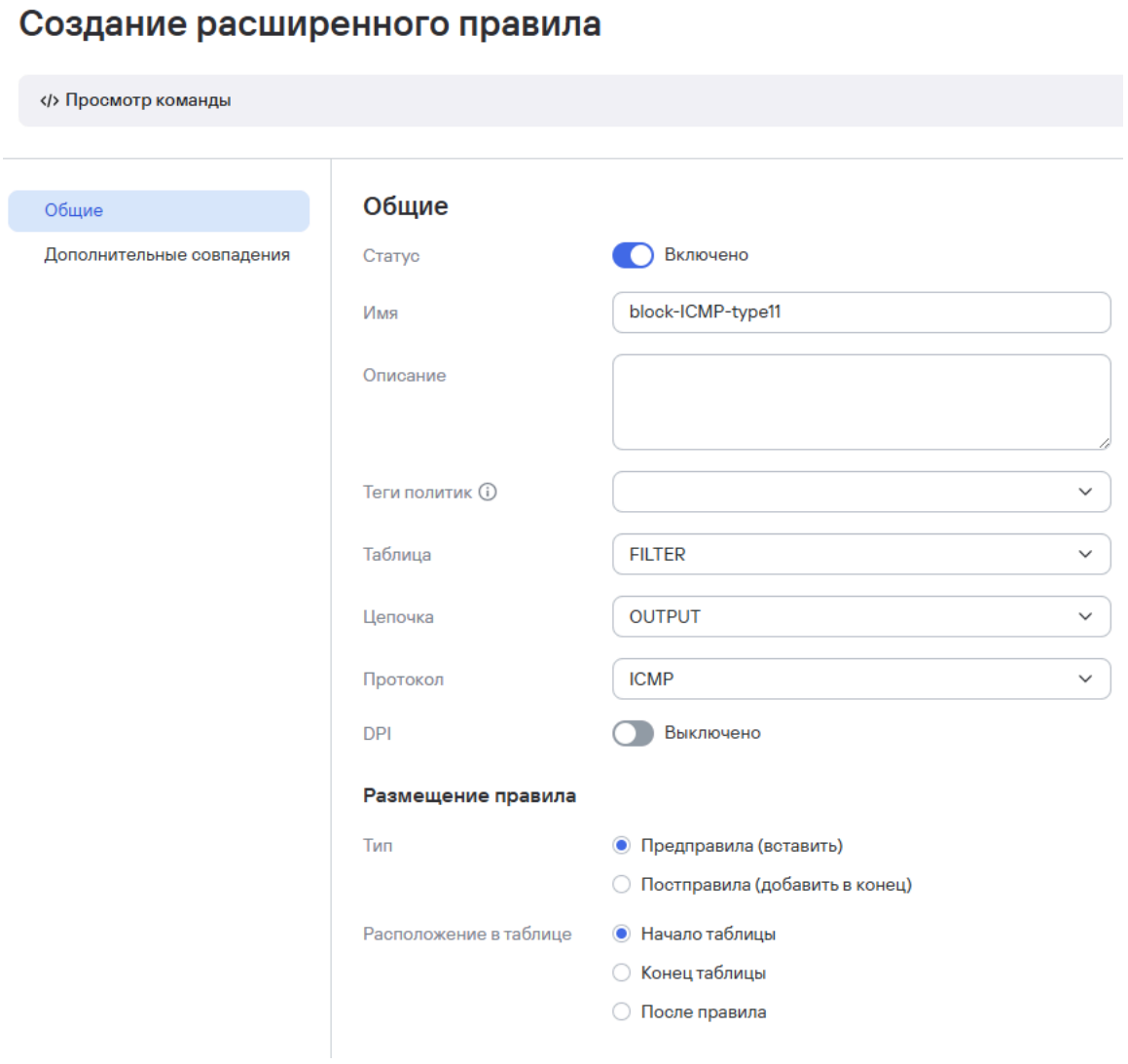
Interpretação:

O que o traceroute faz	Como aparece no tcpdump	O que acontece no CPE
Envia uma solicitação de echo ICMP (ou pacote UDP) com TTL = 1 para o IP 10.123.2.11 de destino (host B).	In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 102...	O roteador recebe o pacote, diminui o TTL para 0, descarta o pacote e retorna uma mensagem ICMP Time-Exceeded à origem.
Recebe uma mensagem ICMP Time-Exceeded do roteador (origem = roteador 10.123.1.1).	Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit...	Este é o primeiro salto na saída do traceroute, o endereço do roteador.
Aumenta o TTL para 2 e envia uma nova solicitação.	In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, seq 103...	TTL = 2 permite que o pacote passe pelo roteador (TTL-1 = 1), mas o roteador ainda não sabe o endereço MAC do host de destino, portanto, ele faz uma solicitação ARP para 10.123.2.11.
Solicitação ARP do roteador (10.123.2.1) → 10.123.2.11.	Out ARP, Request who-has 10.123.2.11 tell 10.123.2.1	O roteador tenta resolver o endereço MAC do host B na segunda sub-rede do roteador.
ARP Reply from 10.123.2.11.	In ARP, Reply 10.123.2.11 is-at bc:24:11:59:58:b7	Depois de obter o endereço MAC do host B, o roteador envia o pacote adiante.
Um pacote com TTL = 2 já alcançou o host de destino (TTL-1 = 1), portanto, o roteador não gera uma mensagem Time-Exceeded, mas simplesmente encaminha o pacote.	Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, seq 105...	O Host B recebe a solicitação e responde com uma resposta de echo ICMP.
Resposta de echo ICMP de 10.123.2.11 → 10.123.1.11.	In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply...	O traceroute recebe a resposta e emite o segundo salto, o endereço do host B.

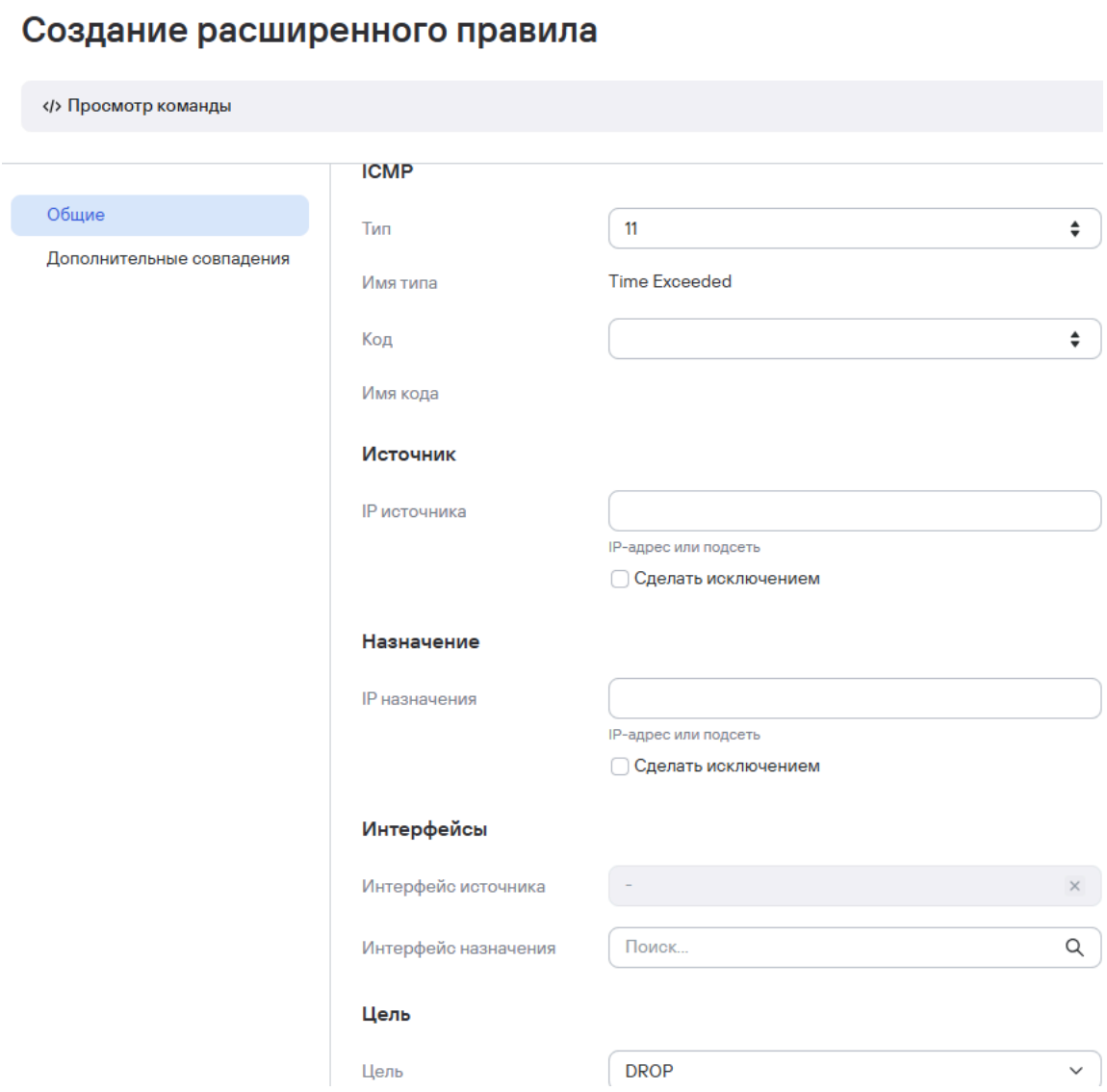
Assim, o cenário para ocultar o dispositivo CPE da detecção na rede envolve as seguintes etapas:

1. **Ocultar o CPE na saída do traceroute**

   a. **Crie uma regra avançada no dispositivo CPE para bloquear mensagens `ICMP Time-Exceeded` de saída geradas no CPE quando ele receber um pacote IP com `TTL=1`:**



Criar uma regra avançada para bloquear mensagens ICMP Time-Exceeded 1



Criar uma regra avançada para bloquear mensagens ICMP Time-Exceeded 2

A regra avançada criada corresponde ao seguinte comando no formato iptables:

```
iptables -t filter -I OUTPUT -p icmp --icmp-type 11 -j DROP -m comment --comment "#ADV Name: block-ICMP-type11"
```

Uma regra semelhante no formato iptables na saída do comando `iptables -L` aparece da seguinte forma:

```
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
DROP icmp -- 0.0.0.0/0 0.0.0.0/0 icmptype 11 /* #ADV Name: block-ICMP-type11 */
```

a. Verifique o rastreamento da rota do host A para o host B:

No host A, faça o rastreamento da rota para o host B:

```
tracert -d 10.123.2.11
```

Resultado:

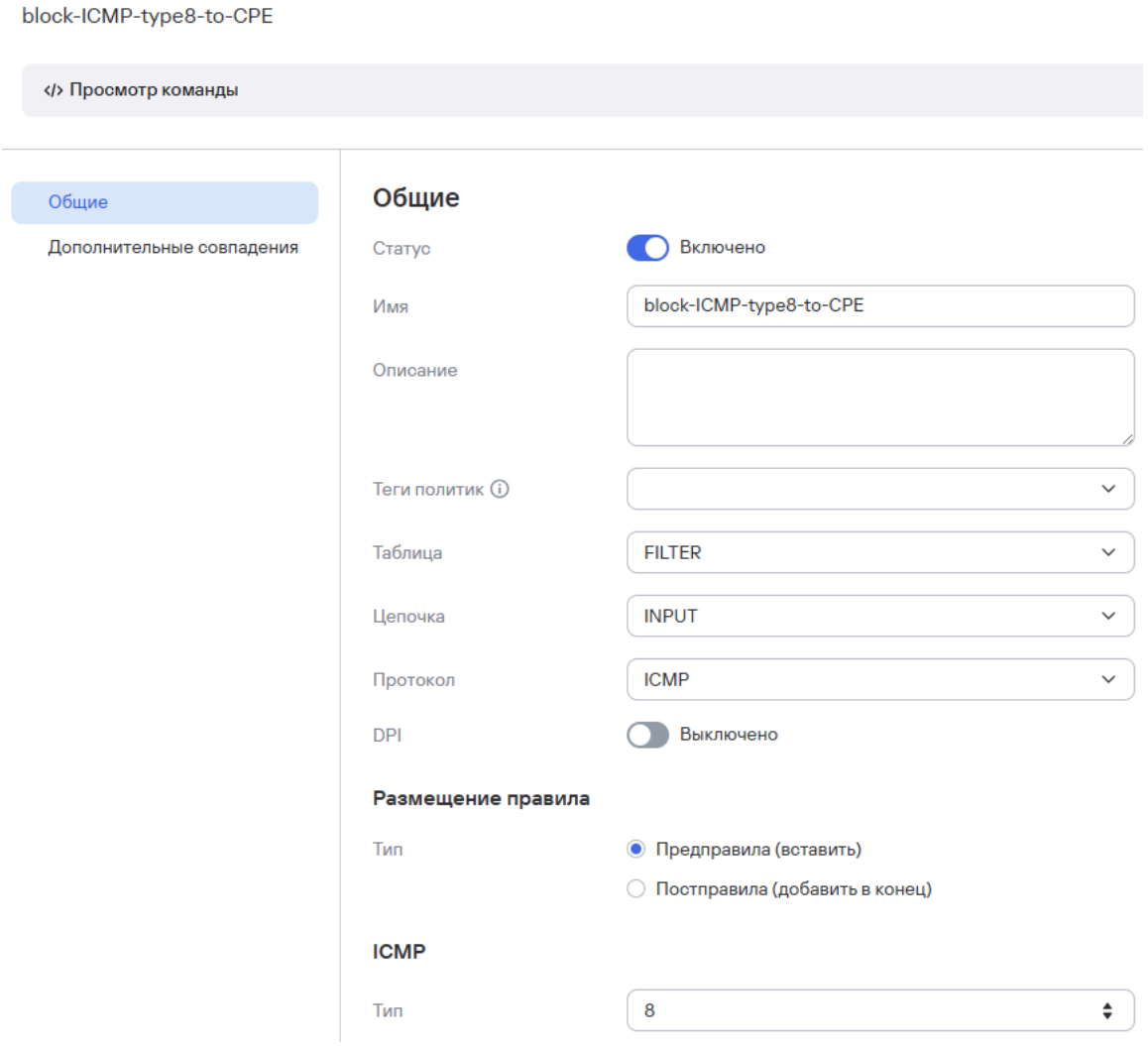
```
1 Request timed out
2 10.123.2.11
```

Interpretação do resultado:

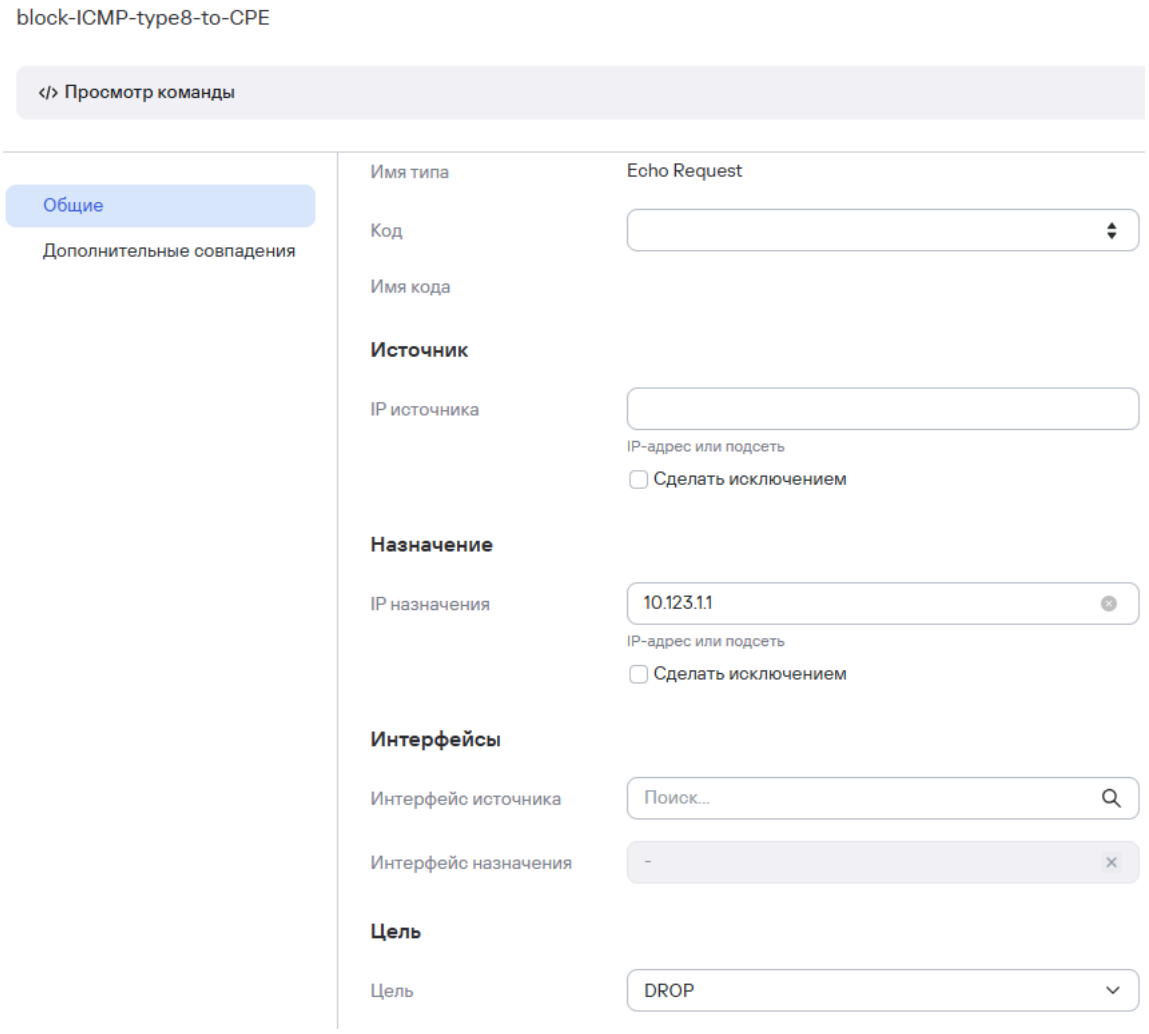
O traceroute envia solicitações de echo ICMP aumentando o TTL. A mensagem `ICMP type 11 (Time-Exceeded)` é gerada pelo roteador, mas é bloqueada pela regra avançada de firewall e, portanto, não aparece no rastreamento. Depois que o host A aumenta o valor de TTL um número suficiente de vezes, o valor se torna suficiente para que a solicitação alcance o host B em `10.123.2.11`, que responde com uma `Resposta de echo` normal. Essa é a única mensagem visível no dump.

2. Bloquear respostas do CPE à solicitação ICMP

a. Crie uma regra estendida no dispositivo CPE que descarta pacotes ICMP vinculados ao dispositivo CPE:



Criar uma regra avançada para descartar pacotes ICMP no CPE (1)



Criar uma regra avançada para descartar pacotes ICMP no CPE (2)

A regra avançada criada corresponde ao seguinte comando no formato iptables:

```
iptables -t filter -I INPUT -p icmp -d 10.123.1.1 --icmp-type 8 -j DROP -m comment --comment "#ADV Name: block-ICMP-type8-to-CPE"
```

Uma regra semelhante no formato iptables na saída do comando iptables -L aparece da seguinte forma:

a. Verifique se a regra funciona: no host A, `execute ping` no endereço do CPE em `eth1`:

```
ping 10.123.1.1
```

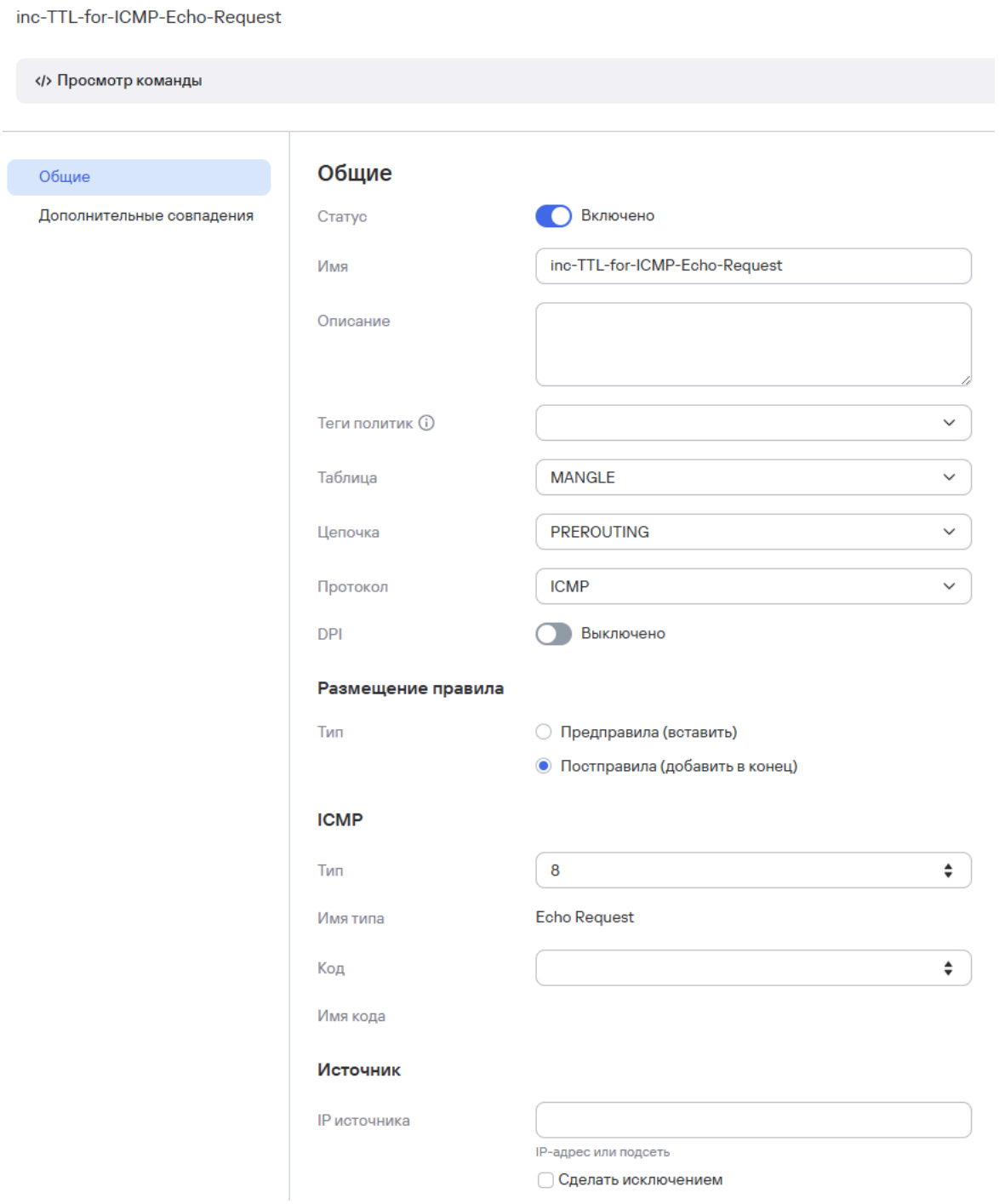
Resultado:

```
Request timed out
```

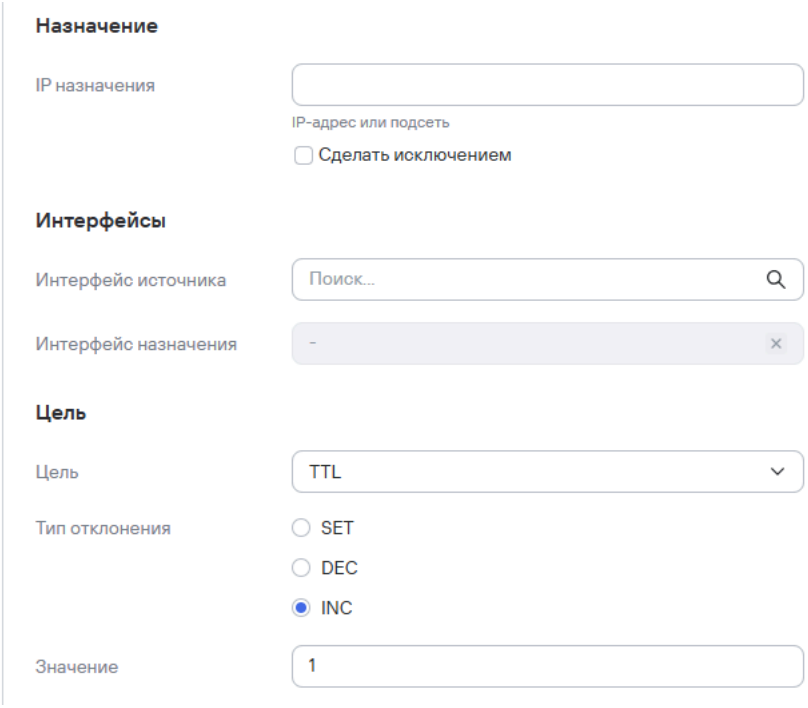
3. Ocultar o CPE do caminho de tráfego usando manipulação de TTL

Você precisa criar uma regra avançada que aumente o TTL de mensagens `ICMP Type 8 (Echo Request)` em 1 antes que o roteador diminua esse valor em 1. Para fazer isso, adicione a regra à cadeia PREROUTING da tabela MANGLE.

a. Crie uma regra avançada no dispositivo CPE que aumente o TTL em 1:



Criar uma regra avançada para aumentar o TTL (1)



Criar uma regra avançada para aumentar o TTL (2)

A regra avançada criada corresponde ao seguinte comando no formato iptables:

```
iptables -t mangle -A PREROUTING -p icmp --icmp-type 8 -j TTL --ttl-inc 1 -m comment --comment "#ADV Name: inc-TTL-for-ICMP-Echo-Request"
```

a. No Host A, rastreie a rota para o Host B.

```
tracert -d 10.123.2.11
```

Resultado:

```
1 10.123.2.11
```

Como esta regra é refletida nos rastreamentos de rotas entre os dois hosts conectados ao CPE:

Etapa	O que acontece sem a regra	O que acontece com a regra
1. O Host A envia um pacote com TTL = 1 (primeiro salto)	O CPE recebe o pacote, diminui o TTL para 0, descarta o pacote e gera uma mensagem ICMP Time-Exceeded (tipo 11) que retorna para A. O host A vê o CPE como o primeiro salto.	Na cadeia PREROUTING, o TTL é aumentado para 2. O CPE então o diminui para 1. O pacote não é descartado e o CPE o envia. Portanto, a mensagem ICMP Time-Exceeded não é gerada e o primeiro salto (CPE) não aparece na saída.
2. O pacote chega ao host de destino (host B)		O pacote chega ao host B com TTL = 1. Aqui o TTL é reduzido para 0 e o Host B gera uma mensagem ICMP Time-Exceeded. O Traceroute mostra o Host B como o primeiro salto.
3. Próximas etapas do traceroute	Nesta etapa, o TTL aumenta para 2, o CPE o diminui para 1. O Host B diminui o TTL para 0, descarta o pacote e gera uma mensagem ICMP Time-Exceeded. O Traceroute mostra o Host B como o segundo salto.	

A regra criada afeta somente pacotes `ICMP tipo 8 (Solicitação de Echo)`. Se o traceroute ou um rastreador de rota semelhante usar pacotes UDP, o primeiro salto ainda estará visível. Para ocultar o roteador do rastreamento de rotas usando pacotes UDP, você precisa criar uma regra semelhante para UDP.

4. **Ocultar informações sobre o fornecedor do dispositivo CPE atribuindo endereços MAC do intervalo LAA às interfaces LAN do dispositivo CPE.**

   Para impedir que os usuários da rede local saibam o fabricante do dispositivo CPE ao observar os endereços MAC padrão de suas interfaces de rede local, você precisa reatribuir endereços MAC do intervalo LAA (Endereço administrado localmente) às interfaces LAN. Um endereço MAC é considerado administrado localmente se o segundo bit menos significativo em seu primeiro octeto for 1. Exemplo:

```
06:1A:2B:3C:4D:5E
06 → 0000 0110
```

Para ocultar informações sobre o fornecedor de um dispositivo CPE:

a. Verifique se o endereço MAC padrão do dispositivo CPE contém informações do fornecedor:

1. No host B, `execute ping` no endereço do gateway (interface `eth2` no CPE com o endereço IP `10.123.2.1`).

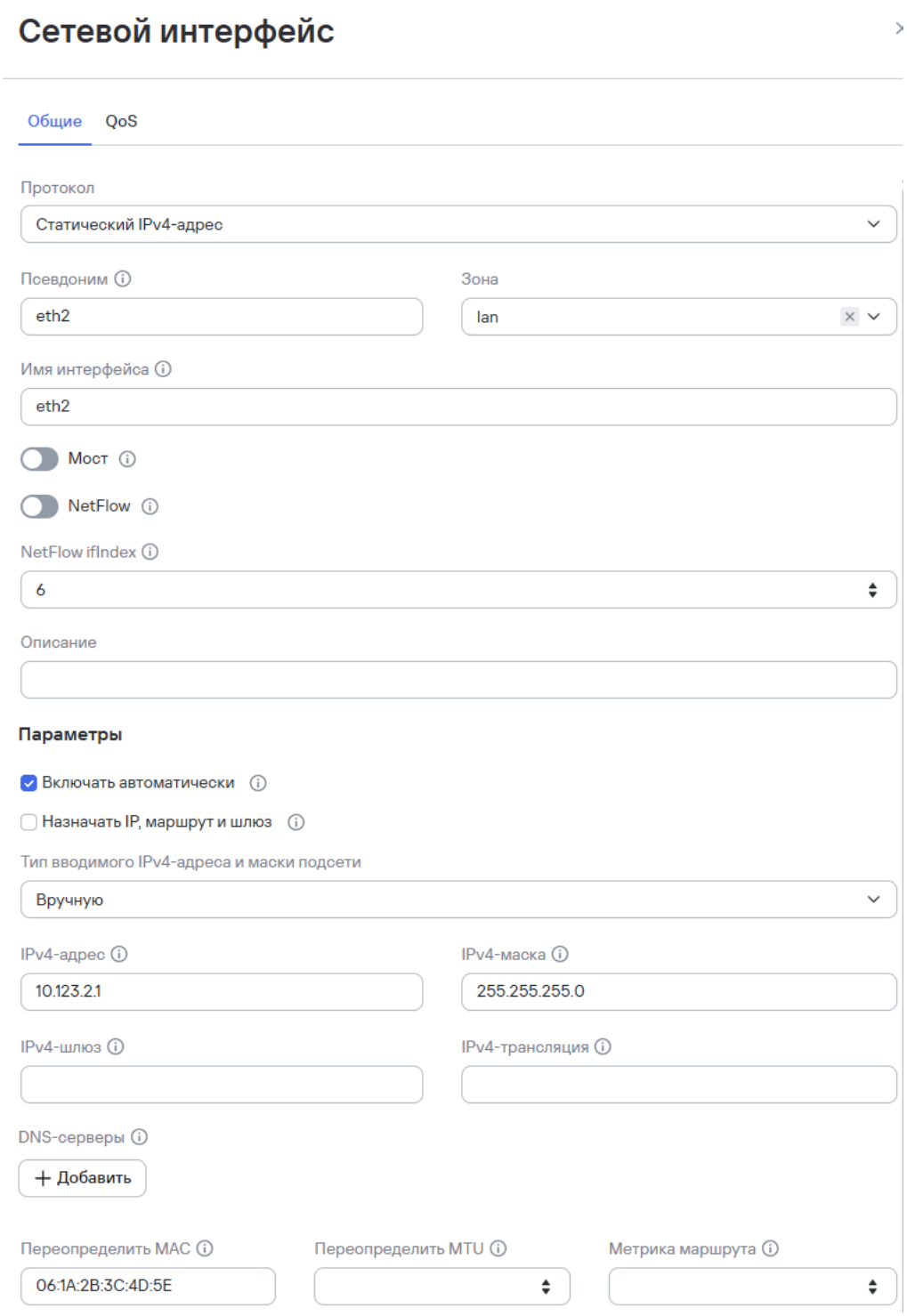
2. Use o WireShark para analisar o tráfego ICMP enviado ao CPE:

```
> Frame 4534: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interf
v Ethernet II, Src: ProxmoxServe_59:58:b7 (bc:24:11:59:58:b7), Dst: ProxmoxServe_57:11:dc
  v Destination: ProxmoxServe_57:11:dc (bc:24:11:57:11:dc)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: ProxmoxServe_59:58:b7 (bc:24:11:59:58:b7)
    Type: IPv4 (0x0800)
    [Stream index: 1]
> Internet Protocol Version 4, Src: 10.123.2.11, Dst: 10.123.2.1
v Internet Control Message Protocol
    Type: Echo (ping) request (8)
    Code: 0
    Checksum: 0x4c0d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 334 (0x014e)
    Sequence Number (LE): 19969 (0x4e01)
    [Response frame: 4535]
  > Data (32 bytes)
```

Análise de tráfego no Wireshark: as informações do fornecedor do CPE são exibidas para o endereço MAC de destino.

No campo `Destino`, o endereço MAC da interface `eth2` do dispositivo CPE é exibido com o prefixo do fornecedor `ProxmoxServe_`. Esse prefixo corresponde aos endereços MAC padrão atribuídos às máquinas virtuais em um ambiente de virtualização Proxmox. Isso permite saber que o dispositivo CPE está sendo executado como uma máquina virtual no ambiente Proxmox. Assim, o aplicativo WireShark foi capaz de determinar o prefixo do fornecedor a partir do endereço MAC padrão.

a. Atribua um endereço MAC do intervalo LLA à interface LAN do dispositivo CPE voltada para o host B (`eth2`):

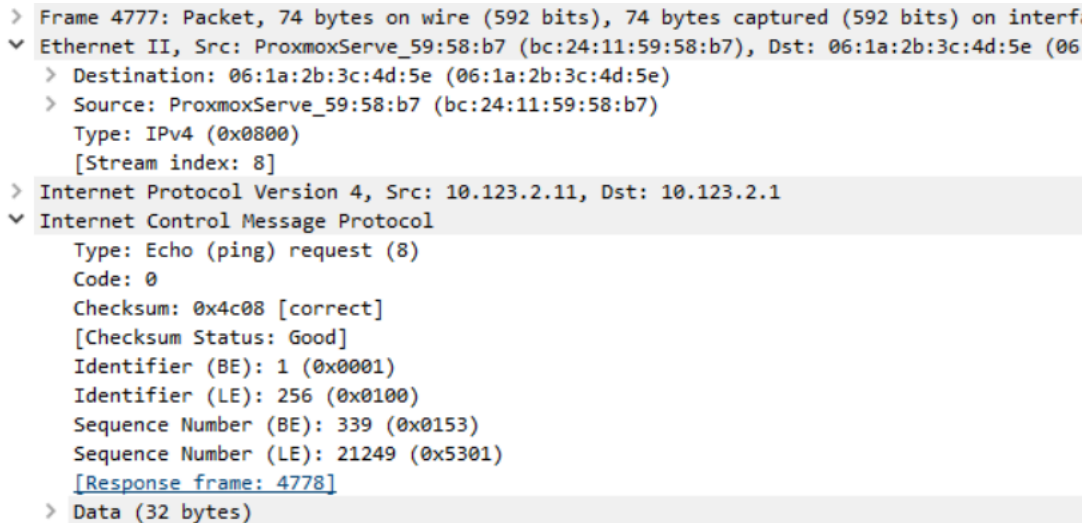


Atribuir um endereço MAC do intervalo LLA à interface LAN do dispositivo

a. Verifique se o endereço MAC padrão do dispositivo CPE não contém informações do fornecedor:

1. No host B, `execute ping` no endereço do gateway novamente (interface `eth2` no CPE com o endereço IP `10.123.2.1`).

2. Use o WireShark para analisar o tráfego ICMP enviado ao CPE:



Análise de tráfego no Wireshark: as informações do fornecedor do dispositivo CPE não são exibidas.

Agora, no campo Destino, o endereço MAC da interface `eth2` do dispositivo CPE é exibido em sua forma original e não indica o ambiente de virtualização ou o fornecedor do equipamento de rede.

Gerenciar conjuntos de IPs

É possível visualizar a tabela de conjuntos de IPs em um modelo de firewall ou um dispositivo CPE:

- Para visualizar a tabela de conjuntos de IPs em um modelo de firewall, vá para a seção **SD-WAN** → **Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Conjuntos de endereços IP**.
- Para visualizar a tabela de conjuntos de IPs em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **Firewall** → **Conjuntos de endereços IP**.

As informações sobre os conjuntos de IPs são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do conjunto de IPs.
- **Correspondência** indica se o conjunto de IPs está associado à origem ou ao destino dos pacotes de tráfego e se o conjunto contém endereços IP ou sub-redes.
- **Entradas** são endereços IP ou sub-redes que foram adicionados ao conjunto de IPs.

Criar um conjunto de IPs

É possível criar um conjunto de IPs em um modelo de firewall ou dispositivo CPE. Conjuntos de IPs criados em um modelo de firewall são criados automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar um conjunto de IPs:

1. Crie um conjunto de IPs de uma das seguintes formas:

   - Para criar um conjunto de IPs em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Conjuntos de endereços IP**.

   - Para criar um conjunto de IPs em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Conjuntos de endereços IP** e marque a caixa de seleção **Substituir**.

   Uma tabela de conjuntos de IPs é exibida.

2. Clique em **+ Conjunto de endereços IP**.

3. Na janela aberta, no campo **Nome**, insira o nome do conjunto de IPs. O comprimento máximo do nome é de 255 caracteres.

4. Na lista suspensa **Direção**, selecione se o conjunto de IPs está associado à origem ou ao destino dos pacotes de tráfego:

   - **Origem correspondente** se o conjunto de IPs contiver endereços IP ou sub-redes de origem.

   - **Destino correspondente** se o conjunto de IPs contiver endereços IP ou sub-redes de destino.

5. Na lista suspensa **Tipo**, selecione se o conjunto contém endereços IP ou sub-redes.

   - **Conjunto de sub-redes** se o conjunto de IPs contiver sub-redes.

   - **Conjunto de IPs** se o conjunto de IPs contiver endereços IP.

6. Se na lista suspensa **Tipo**, tiver sido selecionado **Conjunto de sub-redes**, especifique uma sub-rede. Para isso, em **Lista de entradas**, clique em **+ Adicionar** e insira o prefixo IPv4 da sub-rede. É possível especificar intervalos de octetos de prefixo IPv4 usando colchetes, por exemplo, 192.[165-168].2.0/24.

   A sub-rede é especificada e exibida em **Lista de entradas**. É possível especificar diversas sub-redes ou excluir sub-redes. Para excluir uma sub-rede, clique no ícone de exclusão ✕ ao lado dela.

7. Se na lista suspensa **Tipo**, tiver sido selecionado **Conjunto de IPs**, especifique um endereço IP. Para isso, em **Lista de entradas**, clique em **+ Adicionar** e insira um endereço IPv4. É possível especificar intervalos de octetos de endereço IPv4 usando colchetes, por exemplo, 192.[165-168].2.0.

   O endereço IP é especificado e exibido na seção **Lista de entradas**. É possível especificar diversos endereços IP ou excluir endereços IP. Para excluir um endereço IP, clique no ícone de exclusão ✕ ao lado dele.

8. Clique em **Criar**.

   O conjunto de IPs é criado e exibido na tabela.

9. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Desativar ou ativar um conjunto de IPs

É possível desativar ou ativar um conjunto de IPs em um modelo de firewall ou dispositivo CPE. Um conjunto de IPs ativado ou desativado em um modelo de firewall é ativado ou desativado automaticamente em todos os dispositivos CPE que usam o modelo.

Para desativar ou ativar um conjunto de IPs:

1. Desative ou ative um conjunto de IPs de uma das seguintes formas:

   - Para ativar ou desativar um conjunto de IPs em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Conjuntos de endereços IP**.

   - Para ativar ou desativar um conjunto de IPs em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Conjuntos de endereços IP** e marque a caixa de seleção **Substituir**.

   Uma tabela de conjuntos de IPs é exibida.

2. Clique em **Desativar** ou **Ativar** ao lado do conjunto de IPs que deseja desativar ou ativar.

   O conjunto de IPs é desativado ou ativado.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Editar um conjunto de IPs

É possível editar um conjunto de IPs em um modelo de firewall ou dispositivo CPE. Um conjunto de IPs modificado em um modelo de firewall é modificado automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar um conjunto de IPs:

1. Edite um conjunto de IPs de uma das seguintes formas:

   - Para editar um conjunto de IPs em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Conjuntos de endereços IP**.

   - Para editar um conjunto de IPs em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Conjuntos de endereços IP** e marque a caixa de seleção **Substituir**.

   Uma tabela de conjuntos de IPs é exibida.

2. Clique em **Editar** ao lado do conjunto de IPs que deseja editar.

3. Na janela aberta, se necessário, edite as configurações do conjunto de IPs. Para obter uma descrição das configurações, consulte as instruções para criar um conjunto de IPs.

4. Clique em **Salvar**.

   O conjunto de IPs é modificado e atualizado na tabela.

5. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Excluir um conjunto de IPs

É possível excluir um conjunto de IPs em um modelo de firewall ou dispositivo CPE. Um conjunto de IPs excluído em um modelo de firewall é excluído automaticamente em todos os dispositivos CPE que usam o modelo.

Os conjuntos de IPs excluídos não podem ser restaurados.

Para excluir um conjunto de IPs:

1. Exclua um conjunto de IPs de uma das seguintes formas:

   - Para excluir um conjunto de IPs em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Conjuntos de endereços IP**.
   - Para excluir um conjunto de IPs em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → Conjuntos de endereços IP** e marque a caixa de seleção **Substituir**.

   Uma tabela de conjuntos de IPs é exibida.

2. Clique em **Excluir** ao lado do conjunto de IPs que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   O conjunto de IPs é excluído e não é mais exibido na tabela.

4. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Gerenciar regras de DNAT

Para visualizar a tabela de regras de DNAT em um modelo de firewall ou em um dispositivo CPE:

- Para visualizar a tabela de regras de DNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → DNAT**.
- Para visualizar a tabela de regras de DNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Firewall → NAT → DNAT**.

As informações sobre regras de DNAT são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da regra de DNAT.
- **Entrada** contém os critérios segundo os quais o firewall aplica a regra de DNAT aos pacotes de tráfego:
- **Redirecionamento** é o endereço IP de destino e a porta dos pacotes de tráfego depois que a regra de DNAT é aplicada.

Criar uma regra de DNAT

É possível criar uma regra de DNAT em um modelo de firewall ou em um dispositivo CPE. Regras de DNAT criadas em um modelo de firewall são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma regra de DNAT:

1. Crie uma regra de DNAT de uma das seguintes formas:
   - Para criar uma regra de DNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → DNAT**.
   - Para criar uma regra de DNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → DNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de DNAT é exibida.
2. Clique em **+ DNAT**.
3. Na janela aberta, no campo **Nome**, insira o nome da regra de DNAT. O comprimento máximo do nome é de 255 caracteres.
4. Especifique os critérios segundo os quais o firewall deve aplicar a regra de DNAT aos pacotes de tráfego:
   a. Na lista suspensa **Protocolo**, selecione o protocolo de pacotes de tráfego ao qual o firewall aplica a regra de DNAT:
      - **Endereço IP**.
      - **TCP**.
      - **UDP**.
      - **#** para um protocolo personalizado ou não padrão. Ao selecionar esse valor, no campo **Número do protocolo** exibido, insira o número do protocolo de acordo com o padrão da IANA.
   b. No campo **IP de destino**, insira o endereço IPv4 de destino ou o prefixo dos pacotes de tráfego aos quais o firewall aplica a regra de DNAT.
   c. Para aplicar a regra de DNAT apenas a pacotes de tráfego com a zona de firewall de origem especificada, na lista suspensa **Zona de origem**, selecione uma zona de firewall criada da origem.

d. Caso tenha selecionado **TCP** ou **UDP** na lista suspensa **Protocolo** e desejar aplicar a regra de DNAT apenas a pacotes de tráfego com a porta de destino especificada, insira o número da porta de destino no campo **Porta de destino**. Intervalo de valores: 1 a 65.535.

e. Para aplicar a regra de DNAT apenas a pacotes de tráfego com o endereço ou prefixo IPv4 de origem especificado, no campo **IP de origem**, insira o endereço ou prefixo IPv4 de origem.

5. Especifique como a regra de DNAT modifica os pacotes de tráfego:

   a. No campo **IP de destino**, insira um novo endereço ou prefixo IPv4 de destino.

   b. Na lista suspensa **Zona de destino**, selecione a nova zona de firewall de destino.

   c. Caso tenha selecionado **TCP** ou **UDP** na lista suspensa **Protocolo** e desejar alterar o número da porta de destino dos pacotes de tráfego, insira um novo número de porta de destino no campo **Porta de destino**. Intervalo de valores: 1 a 65.535.

6. Clique em **Criar**.

   A regra de DNAT é criada e exibida na tabela.

7. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Configurar a ordem das regras de DNAT

As regras de DNAT são aplicadas aos pacotes de tráfego em ordem decrescente, começando com a primeira regra de DNAT no topo da tabela. Por padrão, as regras de DNAT são exibidas na tabela na ordem de criação. Regras de DNAT criadas há mais tempo são exibidas mais acima na tabela.

É possível configurar a ordem em que as regras de DNAT são aplicadas em um modelo de firewall ou em um dispositivo CPE. A ordem em que as regras de DNAT são aplicadas, especificada no modelo de firewall, é propagada automaticamente para todos os dispositivos CPE que usam o modelo.

Para configurar a ordem em que as regras de DNAT são aplicadas:

1. Edite a ordem em que as regras de DNAT são aplicadas de uma das seguintes formas:

   - Para configurar a ordem em que as regras de DNAT são aplicadas em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → DNAT**.

   - Para configurar a ordem em que as regras de DNAT são aplicadas em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → DNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de DNAT é exibida.

2. Configure a ordem em que as regras de DNAT são aplicadas clicando nos botões **Para cima** e **Para baixo** ao lado delas.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Desativar ou ativar uma regra de DNAT

É possível desativar ou ativar uma regra de DNAT em um modelo de firewall ou em um dispositivo CPE. Uma regra de DNAT ativada ou desativada em um modelo de firewall é ativada ou desativada automaticamente em todos os dispositivos CPE que usam o modelo.

Para desativar ou ativar uma regra de DNAT:

1. Desative ou ative uma regra de DNAT de uma das seguintes formas:

   - Para desativar ou ativar uma regra de DNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e, na área de configurações exibida, selecione a guia **NAT → DNAT**.

   - Para desativar ou ativar uma regra de DNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu e clique no dispositivo CPE; na área de configurações exibida, selecione a guia **Firewall → NAT → DNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de DNAT é exibida.

2. Clique em **Desativar** ou **Ativar** ao lado da regra de DNAT que deseja desativar ou ativar.

   A regra de DNAT é desativada ou ativada.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Editar uma regra de DNAT

É possível editar uma regra de DNAT em um modelo de firewall ou em um dispositivo CPE. Uma regra de DNAT modificada em um modelo de firewall é modificada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma regra de DNAT:

1. Edite uma regra de DNAT de uma das seguintes formas:

   - Para editar uma regra de DNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → DNAT**.

   - Para editar uma regra de DNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → DNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de DNAT é exibida.

2. Clique em **Editar** ao lado da regra de DNAT que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da regra de DNAT. Para obter uma descrição das configurações, consulte as instruções para criar uma regra de DNAT.

4. Clique em **Salvar**.

   A regra de DNAT é modificada e atualizada na tabela.

5. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Excluir uma regra de DNAT

É possível excluir uma regra de DNAT em um modelo de firewall ou em um dispositivo CPE. Uma regra de DNAT excluída de um modelo de firewall é excluída automaticamente de todos os dispositivos CPE que usam o modelo.

As regras de DNAT excluídas não podem ser restauradas.

Para excluir uma regra de DNAT:

1. Exclua uma regra de DNAT de uma das seguintes formas:

   - Para excluir uma regra de DNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → DNAT**.
   - Para excluir uma regra de DNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → DNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de DNAT é exibida.

2. Clique em **Excluir** ao lado da regra de DNAT que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A regra de DNAT é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Gerenciar regras de SNAT

Para visualizar a tabela de regras de SNAT em um modelo de firewall ou em um dispositivo CPE:

- Para visualizar a tabela de regras de SNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → SNAT**.
- Para visualizar a tabela de grupos de regras de SNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo, selecione a guia **Firewall → NAT → SNAT** e marque a caixa de seleção **Substituir**.

As informações sobre regras de SNAT são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da regra de SNAT.
- **Saída** são critérios segundo os quais o firewall aplica a regra de SNAT a pacotes de tráfego.
- **Ação** é a ação que a regra de SNAT aplica aos pacotes de tráfego.

Criar uma regra de SNAT

É possível criar uma regra de SNAT em um modelo de firewall ou em um dispositivo CPE. Regras de SNAT criadas em um modelo de firewall são criadas automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar uma regra de SNAT:

1. Crie uma regra de SNAT de uma das seguintes formas:
   - Para criar uma regra de SNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → SNAT**.
   - Para criar uma regra de SNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → SNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de SNAT é exibida.
2. Clique em **+ SNAT**.
3. Na janela aberta, no campo **Nome**, insira o nome da regra de SNAT. O comprimento máximo do nome é de 255 caracteres.
4. Especifique os critérios segundo os quais o firewall deve aplicar a regra de SNAT aos pacotes de tráfego:
   a. Na lista suspensa **Protocolo**, selecione o protocolo de pacotes de tráfego ao qual o firewall aplica a regra de SNAT:
      - **TCP**.
      - **UDP**.
      - **IP**.
   b. Na lista suspensa **Zona de destino**, selecione a zona de firewall de destino criada de pacotes de tráfego à qual o firewall aplica a regra de SNAT.
   c. Para aplicar a regra de SNAT apenas a pacotes de tráfego com o endereço ou prefixo IPv4 de origem especificado, no campo **IP de origem**, insira o endereço ou prefixo IPv4 de origem.
   d. Para aplicar a regra de SNAT apenas a pacotes de tráfego com o endereço ou prefixo IPv4 de destino especificado, no campo **IP de destino**, insira o endereço ou prefixo IPv4 de destino.
5. Na lista suspensa **Ação**, selecione **SNAT**.
6. No campo **IP SNAT**, insira um novo endereço ou prefixo IP de origem especificado pela regra de SNAT para pacotes de tráfego.

7. Clique em **Criar**.

   A regra de SNAT é criada e exibida na tabela.

8. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Configurar a ordem das regras de SNAT

As regras de SNAT são aplicadas aos pacotes de tráfego em ordem decrescente, começando com a primeira regra de SNAT no topo da tabela. Por padrão, as regras de SNAT são exibidas na tabela na ordem de criação. Regras de SNAT criadas há mais tempo são exibidas mais acima na tabela.

É possível configurar a ordem em que as regras de SNAT são aplicadas em um modelo de firewall ou em um dispositivo CPE. A ordem em que as regras de SNAT são aplicadas, especificada no modelo de firewall, é propagada automaticamente para todos os dispositivos CPE que usam o modelo.

Para configurar a ordem em que as regras de SNAT são aplicadas:

1. Edite a ordem em que as regras de SNAT são aplicadas de uma das seguintes formas:

   - Para configurar a ordem em que as regras de SNAT são aplicadas em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → SNAT**.

   - Para configurar a ordem em que as regras de SNAT são aplicadas em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → SNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de SNAT é exibida.

2. Configure a ordem em que as regras de SNAT são aplicadas clicando nos botões **Para cima** e **Para baixo** ao lado delas.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Desativar ou ativar uma regra de SNAT

É possível desativar ou ativar uma regra de SNAT em um modelo de firewall ou em um dispositivo CPE. Uma regra de SNAT ativada ou desativada em um modelo de firewall é ativada ou desativada automaticamente em todos os dispositivos CPE que usam o modelo.

Para desativar ou ativar uma regra de SNAT:

1. Desative ou ative uma regra de SNAT de uma das seguintes formas:

   - Para ativar ou desativar uma regra de SNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → SNAT**.

   - Para ativar ou desativar uma regra de SNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → SNAT** e marque a caixa de seleção **Substituir**.

Uma tabela de regras de SNAT é exibida.

2. Clique em **Desativar** ou **Ativar** ao lado da regra de SNAT que deseja desativar ou ativar.

   A regra de SNAT é desativada ou ativada.

3. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Editar uma regra de SNAT

É possível editar uma regra de SNAT em um modelo de firewall ou em um dispositivo CPE. Uma regra de SNAT modificada em um modelo de firewall é modificada automaticamente em todos os dispositivos CPE que usam o modelo.

Para editar uma regra de SNAT:

1. Edite uma regra de SNAT de uma das seguintes formas:

   - Para editar uma regra de SNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → SNAT**.
   - Para editar uma regra de SNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → SNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de SNAT é exibida.

2. Clique em **Editar** ao lado da regra de SNAT que deseja editar.

3. Na janela aberta, se necessário, edite as configurações da regra de SNAT. Para obter uma descrição das configurações, consulte as instruções para criar uma regra de SNAT.

4. Clique em **Salvar**.

   A regra de SNAT é modificada e exibida na tabela.

5. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Excluir uma regra de SNAT

É possível excluir uma regra de SNAT em um modelo de firewall ou em um dispositivo CPE. Uma regra de SNAT excluída de um modelo de firewall é excluída automaticamente de todos os dispositivos CPE que usam o modelo.

As regras de SNAT excluídas não podem ser restauradas.

Para excluir uma regra de SNAT:

1. Exclua uma regra de SNAT de uma das seguintes formas:

   - Para excluir uma regra de SNAT em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **NAT → SNAT**.

   - Para excluir uma regra de SNAT em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall → NAT → SNAT** e marque a caixa de seleção **Substituir**.

   Uma tabela de regras de SNAT é exibida.

2. Clique em **Excluir** ao lado da regra de SNAT que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   A regra de SNAT é excluída e não é mais exibida na tabela.

4. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Gerenciar o encaminhamento

É possível visualizar a tabela de encaminhamentos em um modelo de firewall ou um dispositivo CPE:

- Para visualizar a tabela de encaminhamentos em um modelo de firewall, vá para a seção **SD-WAN → Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Encaminhamento de zona**.

- Para visualizar a tabela de encaminhamentos em um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Firewall → Encaminhamento de zona**.

As informações sobre encaminhamentos são exibidas nas seguintes colunas da tabela:

- **De** é a zona de firewall de saída.

- **Para** é a zona de firewall de entrada.

Criar um encaminhamento

É possível criar um encaminhamento em um modelo de firewall ou em um dispositivo CPE. Encaminhamentos criados em um modelo de firewall são criados automaticamente em todos os dispositivos CPE que usam o modelo.

Para criar um encaminhamento:

1. Crie um encaminhamento de uma das seguintes formas:

   - Para criar um encaminhamento em um modelo de firewall, vá para a seção **SD-WAN** → **Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Encaminhamento de zona**.

   - Para criar um encaminhamento em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall** → **Encaminhamento de zona** e marque a caixa de seleção **Substituir**.

   Uma tabela de encaminhamentos é exibida.

2. Clique em **+ Encaminhamento**.

3. Na janela aberta, na lista suspensa **De**, selecione uma zona de firewall de saída criada.

4. Na lista suspensa **Para**, selecione uma zona de firewall de entrada criada.

5. Clique em **Criar**.

   O encaminhamento é criado e exibido na tabela.

6. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Excluir um encaminhamento

É possível excluir um encaminhamento em um modelo de firewall ou em um dispositivo CPE. Um encaminhamento excluído em um modelo de firewall é excluído automaticamente em todos os dispositivos CPE que usam o modelo.

Os encaminhamentos excluídos não podem ser restaurados.

Para excluir um encaminhamento:

1. Exclua um encaminhamento de uma das seguintes formas:

   - Para excluir um encaminhamento em um modelo de firewall, vá para a seção **SD-WAN** → **Modelos de firewall** do menu, clique no modelo de firewall e selecione a guia **Encaminhamento de zona**.

   - Para excluir um encaminhamento em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE, selecione a guia **Firewall** → **Encaminhamento de zona** e marque a caixa de seleção **Substituir**.

   Uma tabela de encaminhamentos é exibida.

2. Clique em **Excluir** ao lado do encaminhamento que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   O encaminhamento é excluído e não é mais exibido na tabela.

4. Na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de firewall ou dispositivo CPE.

Alterar o modelo de firewall de um dispositivo CPE

Editar o modelo de firewall de um dispositivo CPE pode resultar na perda de comunicação com outros dispositivos CPE, bem como na perda de pacotes de tráfego retransmitidos.

Para alterar o modelo de firewall de um dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ CPE**.

   Uma tabela de dispositivos CPE é exibida.

2. Clique no dispositivo CPE para o qual deseja alterar o modelo de firewall.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, no menu à esquerda é selecionada a seção **Configuração**, que exibe informações gerais sobre o dispositivo CPE. Essa seção também exibe a tabela de tarefas de **Gerenciamento fora da banda** sendo executadas pelo orquestrador.

3. Na lista suspensa **Modelo de firewall**, selecione um modelo de firewall criado.

4. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do dispositivo CPE.

Integração com ferramentas externas de segurança da informação

Você pode integrar uma ferramenta de segurança de informações externa com o Kaspersky SD-WAN para gerenciamento externo de regras de firewall avançadas usando a API do orquestrador. Para integrar ferramentas de segurança da informação externas, crie um usuário local com a função especial **Restricted-API-extern-ISU**, cujas permissões são limitadas a chamar operações de API destinadas ao gerenciamento de regras de firewall avançadas. Um mecanismo de tags de política permite ativar ou desativar regras de firewall avançadas como grupos. Ao criar regras de firewall avançadas, você pode atribuir tags de política a elas e, em seguida, ativar ou desativar todas as regras que tenham uma determinada tag ao mesmo tempo.

Exemplo de uso da tag:
Um usuário cria as seguintes regras avançadas em um modelo de firewall:

1. Recuse o acesso da sub-rede do usuário à sub-rede do servidor de produção com a tag `"user-subnet-compromised"`.

2. Permita o acesso da sub-rede do usuário a todas as sub-redes do servidor.
   A regra 1 tem uma tag e a tag ainda não foi utilizada; portanto, a regra 1 está desativada e os usuários têm permissão para acessar todas as sub-redes com servidores, incluindo servidores de produção.
   Em seguida, sempre que forem detectados indicadores de comprometimento em qualquer estação de trabalho na sub-rede do usuário, uma ferramenta de análise externa (por exemplo, FortiNet NDR ou Kaspersky XDR) chama a API do orquestrador para ativar tags com a tag `"user-subnet-compromised"`.
   O orquestrador ativa a regra 1 na política e todos os dispositivos CPE aos quais esta política se aplica têm essa regra ativada. Como resultado, o acesso do usuário à sub-rede do servidor de produção é bloqueado.

Descrição da API

As chamadas da API devem ser autenticadas e autorizadas.

A autenticação prossegue em três etapas:

1. Faça uma solicitação `GET` para `/api/core/users/current`, receba uma resposta vazia com o status `200/OK` com um cabeçalho que inclui o cookie `CSRF-TOKEN`.

2. Para a autenticação subsequente, faça uma solicitação `POST` para `/api/authentication`, informando os campos `j_username` (nome do usuário) e `j_password` (senha do usuário) no corpo da solicitação, bem como o token obtido na etapa anterior no cabeçalho `X-CSRF-TOKEN`.

3. Para chamadas API subsequentes, o token CSRF deve ser atualizado fazendo uma solicitação `GET` para `/api/core/settings/defpage` e recebendo uma resposta `200/OK` com o novo valor do cookie `CSRF-TOKEN`.

A autorização é executada com base na função da conta de usuário **Restricted-API-extern-ISU**. Os usuários com essa função têm acesso somente às operações da API para ferramentas de segurança da informação externas. Os usuários com outras funções não têm acesso a essas operações da API.

A API para ferramentas de segurança de informações externas inclui as seguintes operações:

Método	Endpoint	Descrição
`GET`	`/api/nfv/sdwan/externalTools/rules`	Obter a configuração de regras de firewall para um modelo de firewall ou dispositivo CPE
`POST`	`/api/nfv/sdwan/externalTools/rules`	Criar uma regra de firewall de uma ferramenta de segurança de informações externa
`DELETE`	`/api/nfv/sdwan/externalTools/rules`	Excluir uma regra de firewall de uma ferramenta de segurança de informações externa pelo nome da regra
`GET`	`/api/nfv/sdwan/externalTools/policyTags`	Obter todas as tags de política para o locatário atual
`PUT`	`/api/nfv/sdwan/externalTools/policyTags`	Atualizar o status da tag de política
`POST`	`/api/nfv/sdwan/externalTools/policyTags`	Criar uma tag de política
`DELETE`	`/api/nfv/sdwan/externalTools/policyTags`	Excluir uma tag de política

Para obter mais informações sobre métodos, consulte a descrição da API do orquestrador.

Gerenciar serviços de rede e virtualização de funções de rede

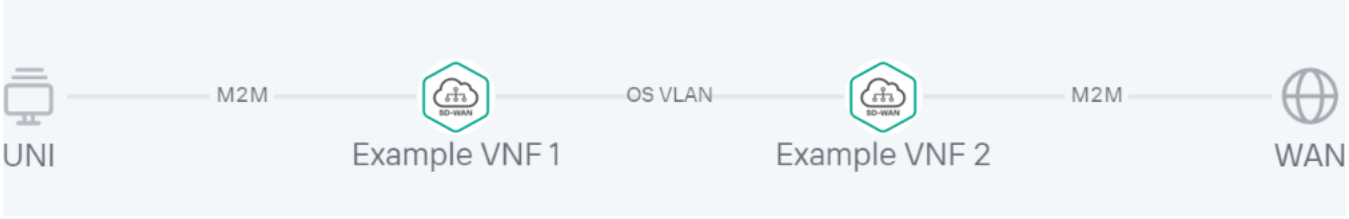
Serviços de rede

Os *serviços de rede* retransmitem o tráfego pela rede e aplicam funções de rede a ele, como otimização de WAN, modelagem e proteção de tráfego. Cada serviço de rede tem uma topologia criada usando uma ferramenta de design gráfico. É possível adicionar componentes de serviço de rede à topologia e conectá-los entre si.

É possível criar uma topologia em um modelo de serviço de rede e atribuir o modelo de serviço de rede a um locatário. Os componentes de serviço de rede adicionados à topologia de modelo são automaticamente atribuídos ao locatário junto com o modelo de serviço de rede. Um locatário pode criar e implementar serviços de rede, se necessário, usando modelos de serviço de rede atribuídos, e editar serviços de rede.

É possível usar os serviços de rede para implementar instâncias SD-WAN. O serviço de rede para implementação de instâncias SD-WAN é chamado de serviço de rede SD-WAN (serviço SD-WAN).

Um exemplo de uma topologia de serviço de rede é mostrado na figura abaixo.



Topologia do serviço de rede

Virtualização de função de rede

A virtualização da função de *rede* (NFV) permite usar armazenamento virtualizado, recursos de computação e redes para fornecer funções de rede e combiná-las em serviços de rede.

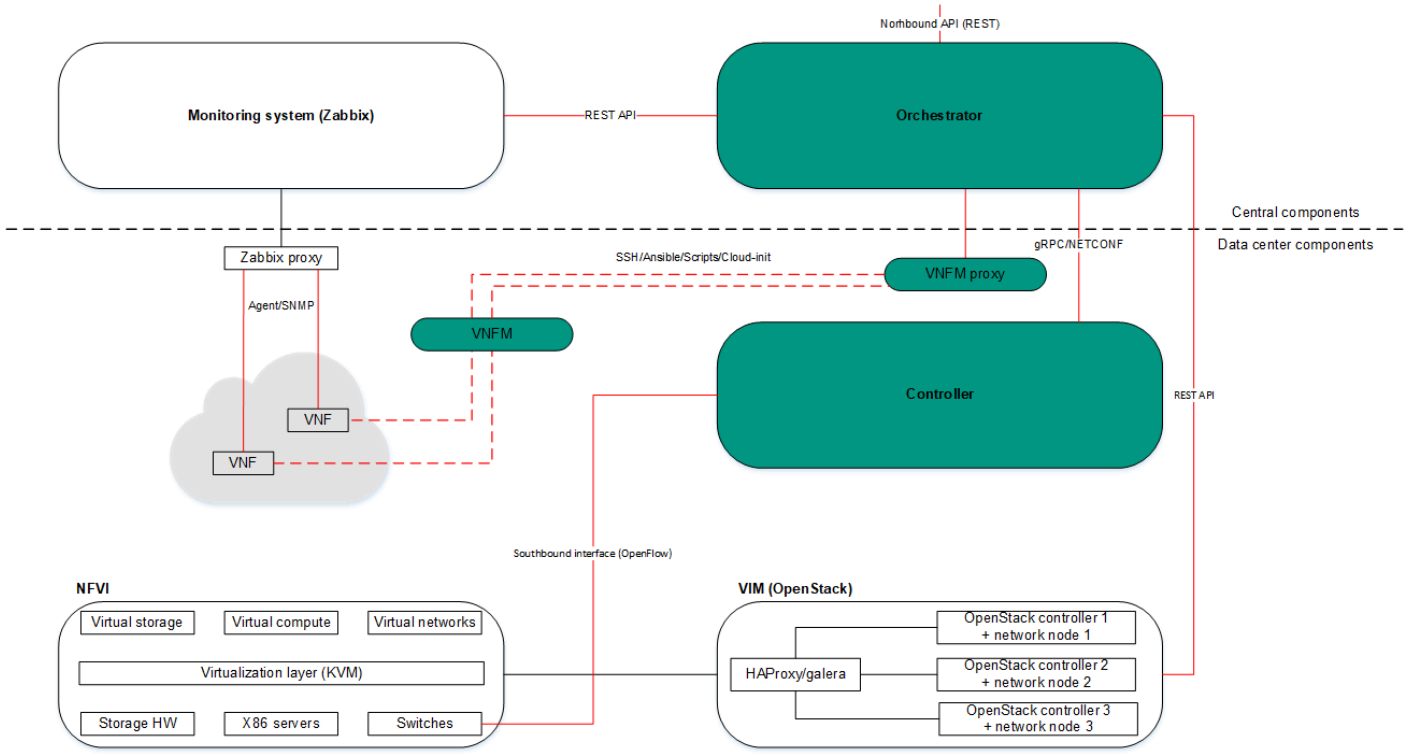
É possível implementar funções de rede virtual (VNF) e funções de rede física (PNF) em serviços de rede. A diferença entre as funções de rede virtual e física é que o orquestrador não gerencia o ciclo de vida das funções de rede física. Há suporte para funções de rede de terceiros.

O Kaspersky SD-WAN está em conformidade com a arquitetura descrita na especificação NFV MANO (Gerenciamento e orquestração de NFV) do ETSI, que define os seguintes componentes funcionais principais:

- Orquestrador.
- Gerenciadores de funções de rede virtual (VNFM).
- Gerenciador de Infraestrutura Virtual.
- O sistema de monitoramento Zabbix monitora o status de funções de rede virtual e funções de rede física e notifica o orquestrador quando uma função de rede precisa ser restaurada ou dimensionada.
- A infraestrutura de NFV abrange recursos físicos, como armazenamento de hardware, servidores e dispositivos de rede.

- Controlador.

A figura abaixo mostra as relações entre os componentes da solução e a infraestrutura de NFV. Os componentes de soluções externas estão marcados em branco, os componentes do Kaspersky SD-WAN estão marcados em verde e as linhas vermelhas são conexões entre componentes.



Infraestrutura NFV

Gerenciar modelos de serviço de rede

É possível visualizar a lista de modelos de serviço de rede no portal do administrador, na seção **Catálogo**, no painel **Catálogo**. Para visualizar informações sobre os componentes disponíveis do serviço de rede, clique no ícone de implementação ». As seguintes subseções são exibidas:

- A guia **Modelos** contém modelos de serviço de rede. As informações sobre modelos de serviço de rede são exibidas nas seguintes colunas da tabela:
  - **Nome** é o nome do modelo de serviço de rede.
  - **Autor** é o nome do usuário que criou o modelo de serviço de rede.
  - **Criado em** é a data e hora em que o modelo de serviço de rede foi criado.
  - **Descrição** é uma breve descrição do modelo de serviço de rede.
- **Serviços de rede compartilhados** é uma lista de serviços de rede compartilhados.

- **Funções de rede virtual** é uma tabela de funções de rede virtual. As informações sobre funções de rede virtual são exibidas nas seguintes colunas da tabela:
  - **Nome** é o nome da função de rede virtual.
  - **Provedor** é o provedor da função de rede virtual. É possível especificar o provedor da função de rede virtual usando o parâmetro `provider` no descritor de VNF.
  - **Versão** é a versão da função de rede virtual. É possível especificar a versão da função de rede virtual usando o parâmetro `version` no descritor de VNF.
  - **Descrição** é a breve descrição da função de rede virtual. É possível especificar uma descrição da função de rede virtual usando o parâmetro `description` no descritor de VNF.
- **Funções de rede física** é a tabela de funções de rede física. As informações sobre as funções físicas da rede são exibidas nas seguintes colunas da tabela:
  - **Nome** é o nome da função de rede física.
  - **Provedor** é o provedor da função de rede física. É possível especificar o provedor da função de rede física usando o parâmetro `provider` no descritor de PNF.
  - **Versão** é a versão da função de rede física. É possível especificar a versão da função de rede física usando o parâmetro `version` no descritor de PNF.
  - **Descrição** é a breve descrição da função de rede física. É possível especificar uma descrição da função de rede física usando o parâmetro `description` no descritor de PNF.

Criar um modelo de serviço de rede

Para criar um modelo de serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. Na parte superior da página, clique em **+ Modelo**.

   A ferramenta de design gráfico para construir a topologia é exibida.

3. Adicione componentes de serviço de rede à topologia:

   a. Arraste os componentes do servidor de rede do painel **Catálogo** para a ferramenta de design gráfico. O painel exibe os seguintes componentes do serviço de rede:

   - Modelos de serviço de rede — ao adicionar um modelo de serviço de rede a uma topologia, a topologia é construída de acordo com o modelo de serviço de rede. É possível adicionar vários modelos de serviço de rede à topologia.
   - Serviços de rede compartilhados — é necessário adicionar um serviço de rede compartilhado à topologia de serviços de rede que se deseja conectar ao serviço de rede compartilhado. É possível especificar uma breve descrição do serviço de rede compartilhado.
   - Funções de rede virtual e física. As ações que podem ser executadas em funções de rede virtual e física são descritas nas seções Gerenciar funções de rede virtual e Gerenciar funções de rede física.

b. Arraste e solte links da guia **Links** para a ferramenta de design gráfico. Os seguintes links são exibidos na guia:

- **P2P** é o serviço de transporte ponto a ponto (serviço P2P). Para configurar um serviço P2P.
- **P2M** é o serviço de transporte ponto a multiponto (serviço P2M). Para configurar um serviço P2M.
- **M2M** é um serviço de transporte multiponto a multiponto (serviço M2M). Para configurar um serviço M2M.

Os links restantes são relevantes para a comunicação de rede no nível do VIM e são estabelecidos entre VNFs hospedados pela plataforma de nuvem OpenStack:

- **SO compartilhado** é a rede compartilhada através da qual o serviço de rede compartilhado conecta-se aos serviços de rede. É possível configurar uma rede compartilhada.
- **Roteador virtual do SO** é o roteador L3 virtual. É possível configurar um roteador virtual.
- **VLAN do SO** é a VLAN para transmissão de tráfego L2 identificado do padrão 802.1Q. É possível configurar uma VLAN.
- **VXLAN do SO** é uma VXLAN para tunelamento. É possível configurar uma VXLAN.
- **SO plano** é a rede simples para transmissão do tráfego L2 não identificado. É possível configurar uma rede simples.

c. Selecione a guia **UNI** e arraste as UNIs do dispositivo CPE para a ferramenta de design gráfico. A guia exibe dois componentes, **UNI** e **WAN**. Ambos designam UNIs abstratas que o locatário deve substituir por UNIs reais ao criar ou editar um serviço de rede. O componente **WAN** se refere às UNIs que se conectam à WAN.

É possível configurar uma UNI na topologia.

Os componentes do serviço de rede são adicionados à topologia e exibidos na ferramenta de design gráfico.

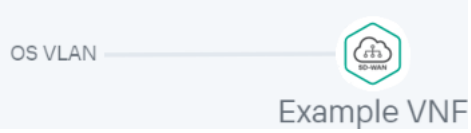
4. Conecte os componentes do serviço de rede adicionados à topologia entre si:

a. Clique no link ao qual deseja conectar um componente de serviço de rede.

b. Clique em **Adicionar folha** para conectar um componente de serviço de rede com a função de folha ao link. Caso tenha clicado em um serviço P2M, clique em **Adicionar raiz** para conectar um componente de serviço de rede com a função raiz ao link.

c. Clique no componente de serviço de rede que deseja conectar ao link. Caso tenha clicado em uma função de rede ou um serviço de rede compartilhado, selecione a porta para conexão do link na janela exibida.

O componente de serviço de rede é conectado ao link e uma linha é exibida entre eles na topologia. Por exemplo, a figura abaixo mostra a VLAN com uma função de rede virtual conectada.



5. Para atribuir UNIs de backup:

Só é possível atribuir uma UNI de backup a UNIs que estejam conectadas a pelo menos um link.

a. Clique na UNI à qual deseja atribuir uma UNI de backup.

b. Clique em **Reservar**.

c. Clique na UNI que deseja usar como backup.

A UNI é designada como UNI de backup e uma linha pontilhada é exibida entre a UNI, a UNI de backup e o link ao qual a UNI está conectada. Por exemplo, na figura abaixo, a WAN é a interface de backup para a UNI.



6. Para remover um componente de serviço de rede da topologia, clique no componente e, em seguida, clique em **Excluir**.

   O componente de serviço de rede é removido da topologia e não é mais exibido na ferramenta de design gráfico.

7. Para alinhar horizontalmente a topologia, clique em **Organizar**.

8. Caso não queira ocultar as descrições dos componentes do serviço de rede adicionados na topologia, desmarque a caixa de seleção **Descrição**. Esta caixa de seleção é selecionada por padrão.

9. No campo **Nome**, insira o nome do serviço de rede.

10. Na parte superior da ferramenta de design gráfico, clique em **Salvar**.

O modelo de serviço de rede é criado e exibido no painel **Catálogo**, na guia **Modelos**.

Editar um modelo de serviço de rede

Ao editar um modelo de serviço de rede, as alterações não são aplicadas aos serviços de rede já criados e implementados usando o modelo de serviço de rede.

Para editar um modelo de serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Catálogo**, selecione a guia **Modelos**.

   Uma lista de modelos de serviço de rede é exibida.

3. Clique no modelo de serviço de rede que deseja editar.

   A ferramenta de design gráfico para construir a topologia é exibida.

4. Se necessário, edite as configurações do modelo de serviço de rede. Para obter uma descrição das configurações, consulte as instruções para criar um modelo de serviço de rede.

5. Na parte superior da ferramenta de design gráfico, clique em **Salvar**.

O modelo de serviço de rede é modificado e atualizado no painel **Catálogo**, na guia **Modelos**.

Excluir um modelo de serviço de rede

Os modelos de serviço de rede excluídos não podem ser restaurados.

Para excluir um modelo de serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Catálogo**, selecione a guia **Modelos**.

   Uma lista de modelos de serviço de rede é exibida.

3. Clique no ícone excluir ✕ ao lado do modelo de serviço de rede que deseja excluir.

4. Na janela de confirmação, clique em **Excluir**.

O modelo de serviço de rede é excluído e não é mais exibido no painel **Catálogo** na guia **Modelos**.

Gerenciar serviços de rede

Antes de gerenciar serviços de rede, faça login no portal de autoatendimento do locatário. A lista de serviços de rede pode ser vista na seção **Catálogo**, no painel **Serviços de rede**. Para ver informações sobre os componentes adicionados à topologia do serviço de rede, clique no serviço e, em seguida, no painel **Objetos**, clique no ícone expandir ». As seguintes subseções são exibidas:

- **VNF** é uma tabela de funções de rede virtual. As informações sobre funções de rede virtual são exibidas nas seguintes colunas da tabela:
  - **Nome** é o nome da função de rede virtual.
  - **Provedor** é o provedor da função de rede virtual. É possível especificar o provedor da função de rede virtual usando o parâmetro `provider` no descritor de VNF.
  - **Versão** é a versão da função de rede virtual. É possível especificar a versão da função de rede virtual usando o parâmetro `version` no descritor de VNF.
  - **Descrição** é a breve descrição da função de rede virtual. É possível especificar uma descrição da função de rede virtual usando o parâmetro `description` no descritor de VNF.

- **Estado** é o estado da função de rede virtual:
  - **PENDING** significa que o estado da função de rede virtual está sendo alterado.
  - **UNDEPLOYED** significa que a função de rede virtual é adicionada à topologia do serviço de rede, mas o serviço de rede não é implementado.
  - **SCHEDULED** significa que a função de rede virtual foi adicionada à topologia do serviço de rede. A implementação de uma função de rede virtual está planejada no dispositivo uCPE, mas não há conexão entre o orquestrador e o dispositivo uCPE. O serviço de rede será implementado quando a comunicação for restaurada.
  - **TERMINATING** significa que a função de rede virtual está sendo removida.
  - **RUNNING** significa que a função de rede virtual está funcionando normalmente.
  - **ERROR** significa que ocorreu um erro ao implementar um serviço de rede com a função de rede virtual em sua topologia.
  - **SCALING** significa que a variação da função de rede virtual está sendo alterada.
  - **HEALING** significa que a recuperação automática da função de rede virtual está em andamento.
  - **DELETED** significa que a função de rede virtual foi excluída.
  - **UPDATING** significa que o serviço de rede com a função de rede virtual em sua topologia está sendo modificado.
  - **REPARING** significa que ocorreu um erro ao modificar o serviço de rede e as configurações anteriores do serviço de rede estão sendo restauradas.
  - **CHECKING** significa que uma verificação de consistência está em andamento para o serviço de rede ao qual a função de rede virtual é adicionada.
  - **DEGRADED** significa que a verificação de consistência do serviço de rede ao qual a função de rede virtual é adicionada revelou a inconsistência da função de rede virtual.
  - **RECOVERING** significa que a função de rede virtual está sendo reimplementada.
- **Autorrecuperação** contém informações sobre se as configurações de recuperação automática de VDU estão especificadas na seção `auto_healing` do pacote de VNF:
  - **Sim**.
  - **Não**.
- **Ajuste de escala automático** contém informações sobre se as configurações de dimensionamento da função de rede virtual estão especificadas na seção `scaling` do pacote de VNF:
  - **Sim**.
  - **Não**.

- **Funções de rede física** é a tabela de funções de rede física. As informações sobre as funções físicas da rede são exibidas nas seguintes colunas da tabela:
  - **Nome** é o nome da função de rede física.
  - **Provedor** é o provedor da função de rede física. É possível especificar o provedor da função de rede física usando o parâmetro `provider` no descritor de PNF.
  - **Versão** é a versão da função de rede física. É possível especificar a versão da função de rede física usando o parâmetro `version` no descritor de PNF.
  - **Descrição** é a breve descrição da função de rede física. É possível especificar uma descrição da função de rede física usando o parâmetro `description` no descritor de PNF.
  - **Estado** é o estado da função de rede física:
    - **PENDING** significa que o estado da função de rede física está sendo alterado.
    - **UNDEPLOYED** significa que a função de rede física é adicionada à topologia do serviço de rede, mas o serviço de rede não é implementado.
    - **TERMINATING** significa que a função de rede física está sendo removida.
    - **RUNNING** significa que a função de rede física está funcionando normalmente.
    - **ERROR** significa que ocorreu um erro ao implementar um serviço de rede com a função de rede física em sua topologia.
    - **SCALING** significa que a variação da função de rede física está sendo alterada.
    - **HEALING** significa que a recuperação automática da função de rede física está em andamento.
    - **DELETED** significa que a função de rede física foi excluída.
    - **UPDATING** significa que o serviço de rede com a função de rede física em sua topologia está sendo modificado.
    - **REPARING** significa que ocorreu um erro ao modificar o serviço de rede e as configurações anteriores do serviço de rede estão sendo restauradas.
    - **CHECKING** significa que uma verificação de consistência está em andamento para o serviço de rede ao qual a função de rede física é adicionada.
    - **DEGRADED** significa que a verificação de consistência do serviço de rede ao qual a função de rede física é adicionada revelou a inconsistência da função de rede física.
    - **RECOVERING** significa que a função de rede física está sendo reimplementada.
  - **Autorrecuperação** contém informações sobre se as configurações de recuperação automática estão especificadas na seção `auto_healing` do pacote de PNF:
    - **Sim**.
    - **Não**.

    - **Ajuste de escala automático** contém informações sobre se as configurações de dimensionamento da função de rede física estão especificadas na seção `scaling` do pacote de PNF:
        - **Sim**.
        - **Não**.
- **Serviço de rede compartilhado** é uma lista de serviços de rede compartilhados.
- **Links** é uma tabela de links. As informações sobre links são exibidas nas seguintes colunas da tabela:
    - **Nome** é o nome do link.
    - **Tipo** é o tipo de link.
    - **Status** é o status do link:
        - **NONE** significa que uma verificação de consistência do serviço de rede ao qual o link é adicionado revelou que o link não existe.
        - **OK** significa que uma verificação de consistência do serviço de rede ao qual o link é adicionado revelou que o link existe.
    - **Compartilhado** indica se a conexão está sendo usada para criar um serviço de rede compartilhado:
        - **Sim**.
        - **Não**.
- **UNI** é uma tabela de UNIs. As informações sobre UNIs são exibidas nas seguintes colunas da tabela:
    - **Nome** é o nome da UNI.
    - **Alias** é o nome da UNI no momento da adição à topologia do serviço de rede.
    - **Status** é o status da UNI:
        - **NONE** significa que uma verificação de consistência do serviço de rede ao qual a UNI é adicionada revelou que a UNI não existe.
        - **OK** significa que uma verificação de consistência do serviço de rede ao qual a UNI é adicionada revelou que a UNI existe.

Criar um serviço de rede

Para criar um serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. Na parte superior do painel **Serviços de rede**, clique em **+ Serviço de rede**.

   A ferramenta de design gráfico para construir a topologia é exibida.

3. Adicione componentes de serviço de rede à topologia:

   a. Arraste os componentes do servidor de rede do painel **Catálogo** para a ferramenta de design gráfico. O painel exibe os seguintes componentes do serviço de rede:

      - Modelos de serviço de rede — ao adicionar um modelo de serviço de rede a uma topologia, a topologia é construída de acordo com o modelo de serviço de rede. É possível adicionar vários modelos de serviço de rede à topologia.

      - Serviços de rede compartilhados — é necessário adicionar um serviço de rede compartilhado à topologia de serviços de rede que se deseja conectar ao serviço de rede compartilhado. É possível especificar uma breve descrição do serviço de rede compartilhado.

      - Funções de rede virtual e física. As ações que podem ser executadas em funções de rede virtual e física são descritas nas seções Gerenciar funções de rede virtual e Gerenciar funções de rede física.

   b. Arraste e solte links da guia **Links** para a ferramenta de design gráfico. Os seguintes links são exibidos na guia:

      - **P2P** é o serviço de transporte ponto a ponto (serviço P2P). Para configurar um serviço P2P.

      - **P2M** é o serviço de transporte ponto a multiponto (serviço P2M). Para configurar um serviço P2M.

      - **M2M** é um serviço de transporte multiponto a multiponto (serviço M2M). Para configurar um serviço M2M.

      Os links restantes são relevantes para a comunicação de rede no nível do VIM e são estabelecidos entre VNFs hospedados pela plataforma de nuvem OpenStack:

      - **SO compartilhado** é a rede compartilhada através da qual o serviço de rede compartilhado conecta-se aos serviços de rede. É possível configurar uma rede compartilhada.

      - **Roteador virtual do SO** é o roteador L3 virtual. É possível configurar um roteador virtual.

      - **VLAN do SO** é a VLAN para transmissão de tráfego L2 identificado do padrão 802.1Q. É possível configurar uma VLAN.

      - **VXLAN do SO** é uma VXLAN para tunelamento. É possível configurar uma VXLAN.

      - **SO plano** é a rede simples para transmissão do tráfego L2 não identificado. É possível configurar uma rede simples.

   c. Selecione a guia **UNI** e arraste as UNIs do dispositivo CPE para a ferramenta de design gráfico. Caso esteja usando um modelo de serviço de rede, substitua as UNIs abstratas na topologia por UNIs reais. UNIs abstratas podem ser designadas por dois componentes, **UNI** e **WAN**. O componente **WAN** se refere às UNIs que se conectam à WAN.

      É possível configurar uma UNI.

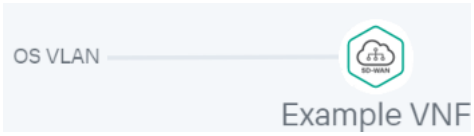
4. Conecte os componentes do serviço de rede adicionados à topologia entre si:

   a. Clique no link ao qual deseja conectar um componente de serviço de rede.

   b. Clique em **Adicionar folha** para conectar um componente de serviço de rede com a função de folha ao link. Caso tenha clicado em um serviço P2M, clique em **Adicionar raiz** para conectar um componente de serviço de rede com a função raiz ao link.

   c. Clique no componente de serviço de rede que deseja conectar ao link. Caso tenha clicado em uma função de rede ou um serviço de rede compartilhado, selecione a porta para conexão do link na janela exibida.

   O componente de serviço de rede é conectado ao link e uma linha é exibida entre eles na topologia. Por exemplo, a figura abaixo mostra a VLAN com uma função de rede virtual conectada.



5. Para atribuir UNIs de backup:

   > Só é possível atribuir uma UNI de backup a UNIs que estejam conectadas a pelo menos um link.

   a. Clique na UNI à qual deseja atribuir uma UNI de backup.

   b. Clique em **Reservar**.

   c. Clique na UNI que deseja usar como backup.

   A UNI é designada como UNI de backup e uma linha pontilhada é exibida entre a UNI, a UNI de backup e o link ao qual a UNI está conectada. Por exemplo, na figura abaixo, a WAN é a interface de backup para a UNI.



6. Para remover um componente de serviço de rede da topologia, clique no componente e, em seguida, clique em **Excluir**.

   O componente de serviço de rede é removido da topologia e não é mais exibido na ferramenta de design gráfico.

7. Para alinhar horizontalmente a topologia, clique em **Organizar**.

8. Caso não queira ocultar as descrições dos componentes do serviço de rede adicionados na topologia, desmarque a caixa de seleção **Descrição**. Esta caixa de seleção é selecionada por padrão.

9. No campo **Nome**, insira o nome do serviço de rede.

10. Conclua a criação do serviço de rede de uma das seguintes formas:

    - Para salvar o serviço de rede, clique em **Salvar**.
    - Para salvar e implementar o serviço de rede, clique em **Implementar**.

    O serviço de rede é criado e exibido no painel **Serviços de rede**. Caso tenha clicado em **Implementar**, a implementação do serviço de rede é iniciada, o que pode levar vários minutos. Para interromper a implementação, clique em **Interromper implementação**.

Editar um serviço de rede

Para editar um serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, selecione o serviço de rede que deseja editar.

   A ferramenta de design gráfico para construir a topologia é exibida.

3. Na parte superior da ferramenta de design gráfico, clique em **Editar**.

4. Se necessário, edite as configurações do serviço de rede. Para obter uma descrição das configurações, consulte as instruções para criar um serviço de rede.

5. Conclua a edição do serviço de rede de uma das seguintes formas:

    - Se estiver editando um serviço de rede não implementado, execute uma das seguintes ações:
        - Para salvar o serviço de rede, clique em **Salvar**.
        - Para salvar e implementar o serviço de rede, clique em **Implementar**.
    - Se estiver editando um serviço de rede implementado, clique em **Implementar mudanças** para implementar o serviço de rede modificado.

    O serviço de rede é modificado e atualizado no painel **Serviços de rede**. Caso tenha clicado em **Implementar** ou **Implementar mudanças**, a implementação é iniciada, o que pode levar vários minutos. Para interromper a implementação, clique em **Interromper implementação**.

Implementando serviço de rede

Se uma função de rede virtual implementada em um dispositivo uCPE for adicionada à topologia do serviço de rede e houver conexão entre o orquestrador e o dispositivo uCPE, o serviço de rede será implementado quando a conexão for restaurada.

Para implementar um serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, selecione o serviço de rede que deseja implementar.

   A ferramenta de design gráfico para construir a topologia é exibida.

3. Na parte superior da ferramenta de design gráfico, clique em **Editar**.

4. Clique em **Implementar**.

   Isso inicia a implementação do serviço de rede, o que pode levar vários minutos. Para interromper a implementação, clique em **Interromper implementação**.

Verificar a consistência de um serviço de rede

A *verificação de consistência* permite confirmar se os componentes adicionados à topologia do serviço de rede realmente existem.

Para verificar a consistência de um serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no ícone de configurações → **Verificar consistência** ao lado do serviço de rede cuja consistência deseja verificar.

3. Na janela de confirmação, clique em **Confirmar**.

   Isso inicia a verificação de consistência do serviço de rede.

Reimplementar um serviço de rede

A reimplementação de um serviço de rede pode resultar em interrupções de curto prazo ou inoperabilidade temporária. Ao planejar atividades de reimplementação, recomendamos considerar as circunstâncias da organização para minimizar as interrupções.

Para reimplementar um serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no ícone de configurações → **Reimplementar** ao lado do serviço de rede que deseja reimplementar.

3. Na janela de confirmação, clique em **Confirmar**.

   Isso inicia a reimplementação do serviço de rede, o que pode levar vários minutos. Para interromper a implementação, clique em **Interromper implementação**.

Desativar ou ativar a recuperação automática para um serviço de rede

O servidor Zabbix monitora os componentes do serviço de rede e envia uma solicitação de API REST ao orquestrador sempre que um problema é detectado. Se a funcionalidade de recuperação automática estiver ativada para o serviço de rede, o orquestrador inicia a recuperação automática para componentes do serviço de rede com problemas. Por padrão, essa funcionalidade está ativada.

Para desativar ou ativar a recuperação automática para um serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no ícone de configurações → **Desativar autorrecuperação** ou **Ativar autorrecuperação** ao lado do serviço de rede para o qual deseja desativar ou ativar a recuperação automática.

   A recuperação automática é desativada ou ativada para o serviço de rede.

É possível executar a recuperação automática de funções de rede virtual ou suas VDUs mesmo se a recuperação automática estiver desativada para o serviço de rede.

Visualizar o log do serviço de rede

Para visualizar o log de um serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no ícone de configurações → **Abrir log** ao lado do serviço de rede cujo log deseja visualizar.

   A página com o log do serviço de rede é exibida.

Excluir um serviço de rede

Os serviços de rede excluídos não podem ser restaurados.

Para excluir um serviço de rede:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no ícone de configurações ⚙ → **Excluir** ao lado do serviço de rede que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

O serviço de rede é excluído e não é mais exibido no painel **Serviços de rede**.

Cenário: implementar uma função de rede virtual

É possível implementar uma função de rede virtual para um locatário em um serviço de rede. O ciclo de vida das funções de rede virtual é gerenciado por um orquestrador. Para implementar funções de rede virtual, é necessário usar a plataforma em nuvem OpenStack.

Por exemplo, você pode implementar uma função de rede virtual no escritório central de sua organização para proteger o tráfego de usuários transmitido entre dispositivos CPE.

A implementação da função de rede virtual envolve as seguintes etapas:

1. **Preparar um pacote de VNF**

   Prepare o pacote de VNF que deseja implementar e, em seguida, carregue o pacote de VNF na interface da Web do orquestrador. Se necessário, ative a proteção de pacotes de VNF e PNF contra substituição antes de carregar o pacote de VNF na interface da Web do orquestrador.

2. **Garantir a conectividade de rede entre o orquestrador e a plataforma de nuvem OpenStack**

   Garanta a conectividade de rede entre a máquina virtual ou o servidor físico onde o orquestrador está implementado e a plataforma de nuvem OpenStack.

3. **Atribuir a função de rede virtual a um locatário**

   Use um dos seguintes métodos para atribuir a função de rede virtual ao locatário para o qual deseja implementá-la:

   - Para implementar uma função de rede virtual usando um modelo de serviço de rede:

     1. Adicione a função de rede virtual à topologia ao criar ou editar um modelo de serviço de rede.

     2. Se necessário, configure a topologia e a função de rede virtual. Para obter uma descrição do que é possível fazer com funções de rede virtual, consulte a seção Gerenciar funções de rede virtual.

     3. Atribua o modelo de serviço de rede a um locatário.

   - Para implementar uma função de rede virtual sem um modelo de serviço de rede, atribua a função de rede virtual ao locatário.

4. **Fazer login no portal de autoatendimento do locatário**

   Faça login no portal de autoatendimento do locatário

5. **Implementar a função de rede virtual**

Faça o seguinte:

1. Adicione a função de rede virtual à topologia ao criar ou editar um serviço de rede de uma das seguintes formas:

   - Para implementar uma função de rede virtual usando um modelo de serviço de rede, adicione o modelo de serviço de rede à topologia.

   - Para implementar uma função de rede virtual sem um modelo de serviço de rede, adicione a função de rede virtual à topologia.

2. Se necessário, configure a topologia e a função de rede virtual. Para obter uma descrição do que é possível fazer com funções de rede virtual, consulte a seção Gerenciar funções de rede virtual.

3. Implemente a função de rede virtual usando um dos seguintes métodos:

   - Caso tenha adicionado a função de rede virtual à topologia ao criar o serviço de rede, implemente o serviço de rede.

   - Caso tenha adicionado a função de rede virtual à topologia ao editar um serviço de rede, implemente o serviço de rede modificado.

A função de rede virtual é implementada.

Cenário: implementar uma função de rede física

É possível implementar uma função de rede física para um locatário em um serviço de rede. Como funções de rede física, podem ser usado um hardware dedicado, bem como entidades virtuais criadas usando ambientes de virtualização de terceiros. O orquestrador não gerencia o ciclo de vida das funções de rede física.

Por exemplo, você pode implementar uma função de rede física no escritório central de sua organização para proteger o tráfego de usuários transmitido entre dispositivos CPE.

A implementação da função de rede física envolve as seguintes etapas:

1. **Preparar o pacote de PNF**

   Prepare o pacote de PNF que deseja implementar e, em seguida, carregue o pacote de PNF na interface da Web do orquestrador. Se necessário, ative a proteção de pacotes VNF e PNF contra substituição antes de carregar o pacote de PNF na interface da Web do orquestrador.

2. **Garantir a conectividade de rede entre o orquestrador e a função de rede física**

   Garanta a conectividade de rede entre a máquina virtual ou o servidor físico em que o orquestrador está implementado e o hardware dedicado ou a entidade virtual em que se deseja implementar a função de rede física.

3. **Atribuir a função de rede física a um locatário**

Use um dos seguintes métodos para atribuir a função de rede física ao locatário para o qual deseja implementá-la:

- Para implementar uma função de rede física usando um modelo de serviço de rede:
  1. Adicione a função de rede física à topologia ao criar ou editar um modelo de serviço de rede.
  2. Se necessário, configure a topologia e a função de rede física. Para obter uma descrição do que é possível fazer com funções de rede física, consulte a seção Gerenciar funções de rede física.
  3. Atribua o modelo de serviço de rede a um locatário.
- Para implementar uma função de rede física sem um modelo de serviço de rede, atribua a função de rede física ao locatário.

4. **Fazer login no portal de autoatendimento do locatário**

   Faça login no portal de autoatendimento do locatário

5. **Implementar uma função de rede física**

   Faça o seguinte:

   1. Adicione a função de rede física à topologia ao criar ou editar um serviço de rede de uma das seguintes formas:
      - Para implementar uma função de rede física usando um modelo de serviço de rede, adicione o modelo de serviço de rede à topologia.
      - Para implementar uma função de rede física sem um modelo de serviço de rede, adicione a função de rede física à topologia.
   2. Se necessário, configure a topologia e a função de rede física. Para obter uma descrição do que é possível fazer com funções de rede física, consulte a seção Gerenciar funções de rede física.
   3. Implemente a função de rede física usando um dos seguintes métodos:
      - Caso tenha adicionado a função de rede física à topologia ao criar o serviço de rede, implemente o serviço de rede.
      - Caso tenha adicionado a função de rede física à topologia ao editar um serviço de rede, implemente o serviço de rede modificado.

A função de rede física é implementada.

Gerenciar pacotes VNF e PNF

Um pacote de *VNF* ou *PNF* é um arquivo ZIP no qual é necessário colocar os seguintes componentes para implementar uma função de rede e gerenciar seu ciclo de vida:

- O descritor de VNF/PNF, um arquivo com parâmetros da função de rede.
- O diretório /image, que contém imagens de máquina virtual no formato QCOW para implementar a função de rede virtual. Esse diretório não está incluído no pacote de PNF.
- O diretório /scripts, que contém scripts para implementar e gerenciar a função de rede.

- logo.png, o ícone da função de rede. Esse componente é opcional.
- description-file.pdf, documentação técnica ou especificação da função de rede. Esse componente é opcional.

É necessário carregar um pacote de VNF ou PNF na interface da Web do orquestrador para implementar uma função de rede virtual ou uma função de rede física.

Configurar o descritor de VNF

Especifique as configurações da função de rede virtual em um descritor de VNF no formato YAML ou XML e, em seguida, adicione o descritor de VNF ao diretório raiz do pacote de VNF. Um descritor VNF tem a seguinte estrutura:

Seção/configuração	Descrição
`name`	Nome da função de rede virtual.
`description`	Breve descrição da função de rede virtual.
`description_file`	Nome do arquivo PDF com a documentação técnica ou a especificação da função de rede virtual. Esse arquivo deve ser colocado no diretório raiz do pacote de VNF. Os usuários podem visualizar e baixar o arquivo na interface da Web do orquestrador. Configuração opcional.
`provider`	Provedor da função de rede virtual.
`version`	Versão da função de rede virtual.
`external_connections`	Pontos de conexão externos da função de rede virtual. É possível configurar os pontos de conexão externos da função de rede virtual especificados na interface da Web do orquestrador.
`internal_connections`	Pontos de conexão internos de VDUs que fazem parte da função de rede virtual. Essa seção é opcional.
`virtual_links`	Links virtuais para conectar pontos de conexão internos. Esta seção deve ser especificada caso a seção `internal_connections` tenha sido especificada.
`images`	Imagens de disco de VDU. É possível implementar várias VDUs usando a mesma imagem de disco de VDU.
`configurations`	Scripts para execução de ações em vários estágios do ciclo de vida da função de rede virtual, por exemplo, durante a implementação da função de rede virtual.
`flavours`	Variações da função de rede virtual. É possível selecionar uma das variações especificadas da função de rede virtual na interface da Web do orquestrador.
`scaling`	Parâmetros de dimensionamento da função de rede virtual. Essa seção é opcional.
`user_configurations`	Entradas da interface da Web do orquestrador que são adicionadas à área de configurações da função de rede virtual. Essa seção é opcional.
`backups`	Tarefas de backup da função de rede virtual. Essa seção é opcional.

Exemplo de descritor de VNF

```
name: OpenWrt18
description: OpenWrt 18.06.1
description_file: openwrt-presentation.pdf
provider: Kaspersky
version: 1.0.1
external_connections:
 - name: LAN
 description: eth1
 ip: AUTO
```

```
 mask: AUTO
 group: eth1-group
 - name: WAN
 description: eth2
 ip: AUTO
 mask: AUTO
 group: eth2-group
images:
 - name: openwrt
 container_format: BARE
 disk_format: QCOW2
 type: OPENSTACK
 filename: openwrt-18.06.1-x86-64.qcow2
configurations:
 - name: config
 filename: config.yml
 stage: initialization
 executor: ansible
 authentication: password
 - name: config2
 filename: 3VDU.sh
 stage: initialization
 executor: /bin/sh
 authentication: key
 - name: config3
 filename: 2VDU.sh
 stage: initialization
 executor: /bin/sh
 authentication: key
flavours:
 - name: 2VDU
 description: 1 vCPU, 512MB memory
 position: 1
 affinity:
 groups:
 - name: aff
 vdu_name:
 - OpenWrt
 - OpenWrt2
 management:
 vnc:
 - vdu_name: OpenWrt
 ssh:
 - vdu_name: OpenWrt
 def_user: root
 authentication: key
 web:
 - vdu_name: OpenWrt
 vdus:
 - name: OpenWrt
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 zabbix_template: Template OS Linux
```

```
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config3
def_user: root
def_password: p@ssw0rd
password_authentication: yes
disks:
- name: default
order: 1
type: default
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
- name: OpenWrt2
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config3
def_user: root
def_password: p@ssw0rd
password_authentication: yes
disks:
- name: default
order: 1
```

```
type: default
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
- name: VDU
description: 1 vCPU, 512MB memory
position: 2
affinity:
groups:
- name: aff
vdu_name:
- OpenWrt
- OpenWrt2
- OpenWrt3
management:
vnc:
- vdu_name: OpenWrt
ssh:
- vdu_name: OpenWrt
def_user: root
authentication: key
web:
- vdu_name: OpenWrt
vdus:
- name: OpenWrt
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
check_connection_mode: none
zabbix_template: Template OS Linux
monitoring_type: agent
```

```
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssword
password_authentication: yes
disks:
- name: default
order: 1
type: default
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
- name: OpenWrt2
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssw0rd
password_authentication: yes
disks:
- name: default
order: 1
type: default
```

```
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
- name: OpenWrt3
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssw0rd
password_authentication: yes
disks:
- name: default
order: 1
type: default
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
```

```
 description: eth0
 - name: eth1
 type: data
 description: eth1
 connection_point_ref: LAN
 - name: eth2
 type: data
 description: eth2
 connection_point_ref: WAN
 auto_healing:
 triggers_set: any
 triggers:
 - name: unreachable
 action_set:
 - type: reprovision
scaling:
 scale_in_status: permit
 scale_out_status: "permit"
user_configurations:
 tab:
 - name: GW
 variables:
 - name: "gw_ip"
 description: IP
 input_type: input
 required: true
 type: string
 default_value: 192.168.0.1
 example: 192.168.0.1
 - name: direction
 description: traffic direction
 input_type: dropdown
 required: true
 type: string
 values:
 - value: in
 is_default: true
 - value: out
 update_configuration_name:
 - update_var
 - change
backups:
 - name: backup_config
 description: backup/etc/config
 backup:
 path: /root/config.thz
 interval: 600
 store_configs: 10
 backup_type: vnfm_scp
 authentication: key
 configuration_name_ref: backup
 restore:
 path: /tmp/config.tgz
 backup_type: vnfm_scp
 authentication: password
 configuration_name_ref: restore
```

external_connections

A seção external_connections tem a seguinte estrutura:

Seção/configuração		Descrição
- name		Nome do ponto de conexão externo.
	description	Breve descrição do ponto de conexão externo.
	ip	Endereço IP do ponto de conexão externo. Insira um valor no formato XXX.XXX.XXX.XXX, por exemplo: 192.168.110.126
	mask	Máscara de sub-rede do ponto de conexão externo. Valores possíveis: • Valor no formato XXX.XXX.XXX.XXX, por exemplo: 255.255.255.0 A máscara de sub-rede é atribuída usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, a máscara de sub-rede não pode ser alterada. • AUTO — A máscara de sub-rede é atribuída automaticamente usando um servidor DHCP externo ou um script da seção configurations. • MANUAL — a máscara de sub-rede deve ser especificada manualmente na interface da Web do orquestrador ao configurar pontos de conexão externos da função de rede virtual.
	gw	Endereço IP do gateway do ponto de conexão externo. Valores possíveis: • Valor no formato XXX.XXX.XXX.XXX, por exemplo: 192.168.110.126 O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • AUTO — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção configurations. • MANUAL — o endereço IP deve ser especificado manualmente na interface da Web do orquestrador ao configurar pontos de conexão externos da função de rede virtual. Configuração opcional.
	dns	Endereço IP do servidor DNS do ponto de conexão externo. Valores possíveis: • Valor no formato XXX.XXX.XXX.XXX, por exemplo: 192.168.110.126 O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • AUTO — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção configurations. • MANUAL — o endereço IP deve ser especificado manualmente na interface da Web do orquestrador ao configurar pontos de conexão externos da função de rede virtual. Configuração opcional.
	group	O grupo ao qual o ponto de conexão externo pertence. Essa configuração é necessária se vários VDUs na função de rede virtual usarem o mesmo ponto de conexão externo.

Exemplo dessa seção

```
external_connections:
- name: LAN
 description: eth1
 ip: 192.168.2.0
 mask: 255.255.255.0
 gw: 192.168.0.1
 dns: 192.168.0.10
 group: lan-group
```

internal_connections

A seção internal_connections tem a seguinte estrutura:

Seção/configuração		Descrição
`- name`		Nome do ponto de conexão interno.
	`description`	Breve descrição do ponto de conexão interno.
	`virtual_link_name`	Nome do link virtual da seção `virtual_links` para o ponto de conexão interno.
	`ip`	Endereço IP do ponto de conexão interno. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • `AUTO` — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção `configurations`. • `MANUAL` — o endereço IP deve ser especificado manualmente na interface da Web do orquestrador ao configurar pontos de conexão externos da função de rede virtual.
	`mask`	Máscara de sub-rede do ponto de conexão interno. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `255.255.255.0` A máscara de sub-rede é atribuída usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, a máscara de sub-rede não pode ser alterada. • `AUTO` — A máscara de sub-rede é atribuída automaticamente usando um servidor DHCP externo ou um script da seção `configurations`.
	`gw`	Endereço IP do gateway do ponto de conexão interno. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • `AUTO` — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção `configurations`. Configuração opcional.
	`dns`	Endereço IP do servidor DNS do ponto de conexão interno. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • `AUTO` — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção `configurations`. Configuração opcional.
	`group`	O grupo ao qual o ponto de conexão interno pertence. Essa configuração é necessária se vários VDUs na função de rede virtual usarem o mesmo ponto de conexão interno.

Exemplo dessa seção

```
internal_connections:
- name: LAN
 description: eth3
 ip: 192.168.2.0
 mask: 255.255.255.0
 gw: 192.168.0.1
 dns: 192.168.0.10
 group: lan-group
 virtual_link_name: int-link
```

virtual_links

A seção `virtual_links` tem a seguinte estrutura:

Seção/configuração		Descrição
`- name`		Nome do link virtual.
	`cidr`	Prefixo IPv4 do link virtual. Insira um valor no formato XXX.XXX.XXX.XXX/XX, por exemplo: `192.168.2.0/24`
	`ip_version`	Versão dos endereços IP na sub-rede. Valores possíveis: • `v4` • `v6`

Exemplo dessa seção

```
virtual_links:
- name: int_link
 cidr: 203.0.113.0/24
 ip_version: v4
```

`images`

A seção `images` tem a seguinte estrutura:

Seção/configuração		Descrição
`- name`		Nome da imagem do disco de VDU.
	`container_format`	Formato do contêiner da imagem do disco de VDU.
	`disk_format`	Formato da imagem do disco de VDU.
	`type`	Tipo VIM.
	`file_name`	Nome do arquivo da imagem do disco de VDU. É necessário colocar a imagem do disco de VDU no diretório /image do pacote de VNF.

Exemplo dessa seção

```
images:
- name: VDU_img
 container_format: BARE
 disk_format: QCOW2
 type: OPENSTACK
 filename: VDU_img.qcow2
```

`configurations`

A seção `configurations` tem a seguinte estrutura:

Seção/configuração		Descrição
`- name`		Nome da função.
	`filename`	O nome do arquivo de script, manual do Ansible ou atributo de dados do usuário para o Cloud-init. É necessário colocar o script no diretório /scripts do pacote de VNF.
	`stage`	O estágio de operação da função de rede virtual em que o script é executado. Valores possíveis: • `initialization` para executar o script na implementação da função de rede virtual. • `termination` para executar o script na exclusão da função de rede virtual. • `none` para executar o script quando um valor for alterado na seção `user_configurations` na área de configurações da função de rede virtual na interface da Web do orquestrador.
	`executor`	Interpretador de scripts. Valores possíveis: • `ansible` • `expect` • `/bin/sh` • `bin/bash` • `cloud-init` • `< caminho para o interpretador de script personalizado >`, por exemplo `/usr/bin/php`
	`authentication`	Método de autenticação do VNFM na função de rede virtual para a execução de scripts. Valores possíveis: • `key` significa que o VNFM é autenticado na função de rede virtual usando uma chave gerada quando a função de rede virtual é implementada. É necessário usar um script para obter a chave, portanto, recomendamos não especificar esse valor para o primeiro script. • `password` significa que o VNFM é autenticado na função de rede virtual com um nome de usuário e senha da seção `flavours` → `vdus`.
	`files_path`	Caminho de arquivos para executar scripts usando SSH. É necessário criar um diretório no diretório /scripts do pacote de VNF e colocar os arquivos nele. Os arquivos são copiados para a VDU. Configuração opcional.
	`config_drive`	Usar o config-drive. Valores possíveis: • `true` • `false` Esse parâmetro deve ser especificado caso `executor` tenha sido especificado como `cloud_init`.
	`timeout`	O tempo de espera para a conclusão do script, em segundos. Se o script não for concluído dentro do tempo especificado, a execução será encerrada. O tempo limite começa no momento em que o script é executado. Especifique esse parâmetro caso tenha especificado um caminho para um executor de script personalizado para o parâmetro `executor`.

Exemplo dessa seção

```
configurations:
 - name: config
 filename: config.yml
 stage: initialization
 executor: ansible
 authentication: password
 files_path: SSH_scripts
 config_drive: true
 timeout: 15
```

`flavours`

A seção `flavours` tem a seguinte estrutura:

Seção/configuração			Descrição
`- name`			Nome da variação.
	`description`		Breve descrição da variação.
	`position`		Número sequencial da variação. A variação com a posição mais baixa tem o desempenho mais baixo.
	`affinity`		Grupos de VDUs hospedados no mesmo host do OpenStack . Recomendamos hospedar VDUs que exijam minimizar os atrasos de comunicação entre si no mesmo host do OpenStack.
	`anti-affinity`		Grupos de VDUs hospedados em diferentes hosts do OpenStack . Recomendamos implementar VDUs que podem exigir dimensionamento vertical ou alta disponibilidade em hosts do OpenStack distintos.
	`management`		Parâmetros dos consoles de administração VDU.
	`vdus`		Configurações de VDU.

As seções `affinity` e `anti-affinity` têm a seguinte estrutura:

Seção/configuração			Descrição
`groups`			Grupos de VDU.
	`- name`		Nome do grupo de VDU.

		`vdu_name`	Nomes dos VDUs. Especifique uma lista de valores, por exemplo:
			`vdu_name:`
			`- VDU_1`
			`- VDU_2`

A seção `management` tem a seguinte estrutura:

Seção/configuração			Descrição
`vnc`			Configurações para gerenciar VDUs usando o console VNC.
	`- vdu_name`		Nome da VDU.
`ssh`			Configurações para gerenciar VDUs usando o console SSH.
	`- vdu_name`		Nome da VDU.
		`def_user`	Nome de usuário para estabelecer a sessão SSH.
		`authentication`	Método de autenticação do VNFM na função de rede virtual para a execução de scripts. Valores possíveis: • `key` significa que o VNFM é autenticado na função de rede virtual usando uma chave gerada quando a função de rede virtual é implementada. É necessário obter a chave usando um script da seção `configurations`. • `password` significa que o VNFM é autenticado na função de rede virtual com um nome de usuário e senha da seção `vdus`.
`web`			Configurações para gerenciar VDUs usando o console da Web.
	`- vdu_name`		Nome da VDU.
		`protocol`	Protocolo para conexão com o console da Web. Valores possíveis: • `http`. • `https`.
		`port`	Porta para conexão com o console da Web. Insira um valor no intervalo de 1 a 65.536. Por padrão, é especificado o número de porta 80.
		`path`	Caminho para o console da Web.
		`def_user`	Nome de usuário para autenticação no console da Web.
		`def_password`	Senha para autenticação no console da Web.

A seção `vdus` tem a seguinte estrutura:

Seção/configuração			Descrição
`- name`			Nome da VDU.
	`password_rules`		Requisitos de senha da VDU. Essa seção é opcional.
		`length`	Comprimento mínimo da senha.
		`use_upper_case`	Os usuários devem usar caracteres maiúsculos na senha. Valores possíveis: • `true` • `false`
		`use_lower_case`	Os usuários devem usar caracteres minúsculos na senha. Valores possíveis: • `true` • `false`
		`use_digits`	Os usuários devem usar numerais na senha. Valores possíveis: • `true` • `false`
		`specific_symbols`	Se os usuários devem usar caracteres especiais na senha, como: `@"!`
		`specific_symbols_min_usage`	Número mínimo de caracteres especiais que devem estar presentes na senha.
	`check_connection_mode`		Tipo de teste de disponibilidade da VDU executado durante a implementação. Por padrão, é executado um teste SSH. Valores possíveis: • `ssh` • `none` Configuração opcional.
	`zabbix_template`		Nome do modelo Zabbix para a VDU.
	`monitoring_type`		Tipo de monitoramento da função de rede virtual. Valores possíveis: • `agent` significa monitorar usando um agente Zabbix. • `snmp` significa monitorar usando o protocolo SNMP.
	`ssh_port`		Número da porta para estabelecer uma sessão SSH. Configuração opcional.
	`ssh_host_key_algorithm`		O algoritmo de chave do host usado. Valores possíveis: • `ssh-rsa`. • `ssh-ed25519`. Recomendamos usar esse algoritmo de chave de host pois ele é criptograficamente forte. Caso essa configuração não seja especificada, o algoritmo ssh-rsa é usado por padrão para compatibilidade com versões anteriores.

	`configurations`		Nomes de scripts da seção `configurations` a serem executados na VDU. Especifique uma lista de valores, por exemplo:
			`vdu_name:`
			`- config_1`
			`- config_2`

	`backups`		Nomes das tarefas de backup dos `backups` a serem usados na VDU. Especifique uma lista de valores, por exemplo:
			`vdu_name:`
			`- backup_1`
			`- backup_2`
			Essa seção é opcional.

	`def_user`		Nome de usuário para autenticar o VNFM na função de rede virtual. Configuração opcional.
	`def_password`		Senha para autenticar o VNFM na função de rede virtual. Configuração opcional.
	`password_authentication`		Autenticação de senha do VNFM na função de rede virtual. Valores possíveis: • `sim` • `Não` Configuração opcional.

Seção/configuração			Descrição
`disks`			Parâmetros de discos virtuais de VDU.
	`- name`		Nome do disco virtual de VDU.
		`order`	Ordem de montagem do disco virtual de VDU.
		`type`	Tipo do disco efêmero do OpenStack.
		`image`	Nome da imagem do disco virtual de VDU da seção `images`. Parâmetro opcional caso esteja criando um disco de VDU em branco.
		`storage_db`	Tamanho do disco virtual de VDU em gigabytes.
`cpu`			Parâmetros da CPU da VDU.
	`smt`		Requisitos de multithreading simultâneo para implementação da VDU. Valores possíveis: • `prefer`, para usar multithreading simultâneo se estiver ativado no host da VDU. • `isolate` para não usar multithreading simultâneo. • `require` para usar multithreading simultâneo.
	`cpu_pinning`		Uso de anexação da CPU. Valores possíveis: • `shared` para não anexar os núcleos da CPU à VDU. • `dedicated` para anexar os núcleos da CPU à VDU.
	`num_vpu`		Número de núcleos de CPU fixados à VDU.
`memory`			Configurações de RAM da VDU.
	`total_memory_mb`		Quantidade de RAM da VDU, em megabytes.
	`page_size`		Tamanho das páginas de memória ao implementar a VDU. Valores possíveis: • `small` para 4 KB • `large` para 2 MB ou 1 GB • `qualquer` para qualquer tamanho • `4 KB` • `2 MB` • `2048` • `1 GB`
`network_interfaces`			Configurações da interface de rede
	`- name`		Nome da interface de rede.
		`type`	Tipo da interface de rede. Valores possíveis: • `data` é uma interface de rede para transferência de dados. • `management` é uma interface de rede de gerenciamento mapeada para uma porta de rede.
		`description`	Breve descrição da interface de rede.
		`connection_point_ref`	Nome do ponto de conexão externo da seção `external_connections` para a interface de rede de gerenciamento.
		`port_security`	Se a segurança de portas é usada. Valores possíveis: • `disabled` • `enabled` Configuração opcional.
		`properties`	Configurações avançadas da interface de rede.
		`vnic_type`	Tipo de vNIC da interface de rede. Valores possíveis: • `virtio` • `direct` • `macvtap` • `vhost`
`auto_healing`			Parâmetros de recuperação automática da VDU.

Seção/configuração				Descrição
		`triggers_set`		Acionadores externos que iniciam a recuperação automática da VDU. Valores possíveis: • `any` para que qualquer acionador externo inicie a recuperação automática da VDU. • `all` para iniciar a recuperação automática da VDU se todos os acionadores externos especificados forem acionados. • `< nome do acionador >` para iniciar a recuperação automática da VDU quando o acionador externo especificado for acionado.
		`triggers`		Acionadores externos.
			`- name`	Nome do acionador externo. Valores possíveis: • `unreachable` • `scale_up` • `scale_down`
		`action_set`		Ação a ser executada quando um acionador externo é acionado.
			`- type`	Tipo de ação. Valores possíveis: • `reprovision` para reprovisionar a VDU. • `reboot` para reiniciar a VDU. • `script` para executar o script especificado.
			`configuration_name_ref`	Nome do script da seção `configurations` executado quando um acionador externo é acionado. Esse parâmetro deve ser especificado caso `script` tenha sido selecionado como `- type`.
	`bootstrap_timeout`			Tempo limite de disponibilidade do SSH durante a implementação da VDU, em segundos. Se a VDU não estiver disponível através do SSH após o tempo limite especificado, a implementação será revertida. Configuração opcional.

Exemplo dessa seção

```
vdus:
 - name: vgw
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 check_connection_mode: none
 zabbix_template: Template OS Linux
 monitoring_type: agent
 ssh_port: 22
 configurations:
 - config_1
 - config_2
 backups:
 - backup_config
 def_user: root
 def_password: p@ssw0rd
 password_authentication: yes
 disks:
 - name: "default"
 order: 1
 type: default
 image: openwrt
 storage_gb: 1
 cpu:
```

```
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
page_size: small
network_interfaces:
- name: eth
type: data
description: eth0
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
```

scaling

A seção `scaling` tem a seguinte estrutura:

Configuração	Descrição
`scale_in_status`	Dimensionamento horizontal para uma variação com um número sequencial mais baixo. Valores possíveis: • `permit` • `deny`
`scale_out_status`	Dimensionamento horizontal para uma variação com um número sequencial mais alto. Valores possíveis: • `permit` • `deny`
`scale_up_status`	Dimensionamento vertical para uma variação com um número sequencial mais baixo. Valores possíveis: • `permit` • `deny`
`scale_down_status`	Dimensionamento vertical para uma variação com um número sequencial mais alto. Valores possíveis: • `permit` • `deny`

Exemplo dessa seção

```
scaling:
 scale_in_status: permit
 scale_out_status: permit
 scale_up_status: permit
 scale_down_status: permit
```

user_configurations

A seção `user_configurations` tem a seguinte estrutura:

Seção/configuração	Descrição
`tab`	Guias adicionadas à área de configurações da função de rede virtual.
`- name`	Nome da guia.

Seção/configuração			Descrição
	`variables`		Entradas da interface da Web do orquestrador que são exibidas na guia.
	`- name`		Nome da entrada da interface da Web do orquestrador.
		`description`	Breve descrição da entrada da interface da Web do orquestrador.
		`input_type`	Tipo de entrada da interface da Web do orquestrador. Valores possíveis: • `input` para adicionar um campo. • `dropdown` para adicionar uma lista suspensa.
		`default_value`	Valor padrão do campo. É possível especificar esse parâmetro caso `input` tenha sido especificado como `input_type`.
		`values`	As opções exibidas na lista suspensa. É possível especificar essa configuração caso `dropdown` tenha sido especificado como `input_type`.
		`- value`	O nome do valor.
		`is_default`	Valor padrão. Valores possíveis: • `true` • `false` Configuração opcional.
		`required`	Entrada obrigatória da interface da Web do orquestrador. Valores possíveis: • `true` • `false` Configuração opcional.
		`type`	Tipo de valor que pode ser especificado na entrada da interface da Web do orquestrador. Configuração opcional.
		`example`	Uma dica de ferramenta exibida quando o valor da entrada da interface da Web do orquestrador é alterado. Configuração opcional.

		`update_configuration_name`	Nomes de scripts da seção `configurations` executados quando o valor da entrada da interface da Web do orquestrador é alterado. Especifique uma lista de valores, por exemplo:
			`update_configuration_name:`
			`- config_1`
			`- config_2`

Exemplo dessa seção

```
user_configurations:
 tab:
 - name: GW
 variables:
 - name: "gw_ip"
 description: IP
 input_type: input
 required: true
 type: string
 default_value: 192.168.0.1
 example: 192.168.0.1
 - name: direction
 description: traffic direction
 input_type: dropdown
 required: true
 type: string
 values:
 - value: in
 is_default: true
```

```
- value: out
update_configuration_name:
- update_var
- change
```

backups

A seção backups tem a seguinte estrutura:

Seção/configuração			Descrição
- name			Nome da tarefa de backup.
	description		Breve descrição da tarefa de backup.
	backup		Parâmetros de backup.
		path	Caminho para o diretório da função de rede virtual onde os para backup estão localizados.
		interval	Intervalo de tempo em segundos para o backup.
		store_config	Número de cópias de backup a serem mantidas.
		backup_type	Tipo de backup.
		authentication	Método de autenticação do VNFM na função de rede virtual para a execução de scripts. Valores possíveis: • key significa que o VNFM é autenticado na função de rede virtual usando uma chave gerada quando a função de rede virtual é implementada. É necessário obter a chave usando um script da seção configurations. • password significa que o VNFM é autenticado na função de rede virtual com um nome de usuário e senha da seção flavours → vdus.
		configuration_name_ref	Nome do script da seção configurations a ser executado antes do backup.
	restore		Parâmetros de restauração de backup.
		path	Caminho para o diretório da função de rede virtual onde os arquivos restaurados são colocados.
		backup_type	Tipo de backup.
		authentication	Método de autenticação do VNFM na função de rede virtual para a execução de scripts. Valores possíveis: • key significa que o VNFM é autenticado na função de rede virtual usando uma chave gerada quando a função de rede virtual é implementada. É necessário obter a chave usando um script da seção configurations. • password significa que o VNFM é autenticado na função de rede virtual com um nome de usuário e senha da seção flavours → vdus.
		configuration_name_ref	Nome do script da seção configurations a ser executado após o início da restauração a partir do backup.

Exemplo dessa seção

```
backups:
 - name: backup_config
 description: backup/etc/config
 backup:
 path: /root/config.thz
 interval: 600
 store_configs: 10
 backup_type: vnfm_scp
 authentication: key
 configuration_name_ref: backup
 restore:
 path: /tmp/config.tgz
```

```
backup_type: vnfm_scp
authentication: password
configuration_name_ref: restore
```

Configurar o descritor de PNF

Especifique as configurações da função de rede física em um descritor de PNF no formato YAML ou XML e, em seguida, adicione o descritor de PNF ao diretório raiz do pacote de PNF. Um descritor de PNF tem a seguinte estrutura:

Seção/configuração	Descrição
`name`	Nome da função de rede física.
`description`	Breve descrição da função de rede física.
`description_file`	Nome do arquivo PDF com a documentação técnica ou a especificação da função de rede física. Esse arquivo deve ser colocado no diretório raiz do pacote de PNF. Os usuários podem visualizar e baixar o arquivo na interface da Web do orquestrador. Configuração opcional.
`provider`	Provedor da função de rede física.
`version`	Versão da função de rede física.
`external_connections`	Pontos de conexão externos da função de rede física.
`internal_connections`	Pontos de conexão interna de VDUs que fazem parte da função de rede física. Essa seção é opcional.
`configurations`	Scripts para execução de ações em vários estágios do ciclo de vida da função de rede física, por exemplo, durante a implementação da função de rede física.
`flavours`	Variações da função de rede física. É possível selecionar uma das variações especificadas da função de rede física na interface da Web do orquestrador.
`scaling`	Parâmetros de dimensionamento da função de rede física. Essa seção é opcional.
`user_configurations`	Entradas da interface da Web do orquestrador que são adicionadas à área de configurações da função de rede física. Essa seção é opcional.
`backups`	Tarefas de backup da função de rede física. Essa seção é opcional.

Descritor de PNF

```
name: OpenWrt18
description: OpenWrt 18.06.1
description_file: openwrt-presentation.pdf
provider: Kaspersky
version: 1.0.1
external_connections:
 - name: LAN
 description: eth1
 ip: AUTO
 mask: AUTO
 group: eth1-group
 - name: WAN
 description: eth2
 ip: AUTO
 mask: AUTO
 group: eth2-group
configurations:
```

```
 - name: config
 filename: config.yml
 stage: initialization
 executor: ansible
 authentication: password
 - name: config2
 filename: 3VDU.sh
 stage: initialization
 executor: /bin/sh
 authentication: key
 - name: config3
 filename: 2VDU.sh
 stage: initialization
 executor: /bin/sh
 authentication: key
flavours:
 - name: 2VDU
 description: 1 vCPU, 512MB memory
 position: 1
 management:
 ssh:
 - vdu_name: OpenWrt
 def_user: root
 authentication: key
 web:
 - vdu_name: OpenWrt
 vdus:
 - name: OpenWrt
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 zabbix_template: Template OS Linux
 monitoring_type: agent
 ssh_port: 22
 configurations:
 - config
 - config3
 def_user: root
 def_password: p@ssw0rd
 password_authentication: yes
 network_interfaces:
 - name: Management
 type: management
 description: eth0
 - name: eth1
 type: data
 description: eth1
 connection_point_ref: LAN
 - name: eth2
 type: data
 description: eth2
 connection_point_ref: WAN
 auto_healing:
 triggers_set: any
```

```
triggers:
- name: unreachable
action_set:
- type: reboot
- name: OpenWrt2
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config3
def_user: root
def_password: p@ssw0rd
password_authentication: yes
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reboot
- name: VDU
description: 1 vCPU, 512MB memory
position: 2
management:
ssh:
- vdu_name: OpenWrt
def_user: root
authentication: key
web:
- vdu_name: OpenWrt
vdus:
- name: OpenWrt
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
```

```
check_connection_mode: none
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssword
password_authentication: yes
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reboot
- name: OpenWrt2
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssw0rd
password_authentication: yes
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
```

```
 triggers_set: any
 triggers:
 - name: unreachable
 action_set:
 - type: reboot
 - name: OpenWrt3
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 zabbix_template: Template OS Linux
 monitoring_type: agent
 ssh_port: 22
 configurations:
 - config
 - config2
 def_user: root
 def_password: p@ssw0rd
 password_authentication: yes
 network_interfaces:
 - name: Management
 type: management
 description: eth0
 - name: eth1
 type: data
 description: eth1
 connection_point_ref: LAN
 - name: eth2
 type: data
 description: eth2
 connection_point_ref: WAN
 auto_healing:
 triggers_set: any
 triggers:
 - name: unreachable
 action_set:
 - type: reboot
scaling:
 scale_in_status: permit
 scale_out_status: "permit"
user_configurations:
 tab:
 - name: GW
 variables:
 - name: "gw_ip"
 description: IP
 input_type: input
 required: true
 type: string
 default_value: 192.168.0.1
 example: 192.168.0.1
 - name: direction
 description: traffic direction
 input_type: dropdown
 required: true
```

```
 type: string
 values:
 - value: in
 is_default: true
 - value: out
 update_configuration_name:
 - update_var
 - change
backups:
 - name: backup_config
 description: backup/etc/config
 backup:
 path: /root/config.thz
 interval: 600
 store_configs: 10
 backup_type: vnfm_scp
 authentication: key
 configuration_name_ref: backup
 restore:
 path: /tmp/config.tgz
 backup_type: vnfm_scp
 authentication: password
 configuration_name_ref: restore
```

external_connections

A seção external_connections tem a seguinte estrutura:

Seção/configuração		Descrição
`- name`		Nome do ponto de conexão externo.
	`description`	Breve descrição do ponto de conexão externo.
	`ip`	Endereço IP do ponto de conexão externo. Insira um valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126`
	`mask`	Máscara de sub-rede do ponto de conexão externo. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `255.255.255.0` A máscara de sub-rede é atribuída usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, a máscara de sub-rede não pode ser alterada. • `AUTO` — A máscara de sub-rede é atribuída automaticamente usando um servidor DHCP externo ou um script da seção `configurations`.
	`gw`	Endereço IP do gateway do ponto de conexão externo. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • `AUTO` — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção `configurations`. Configuração opcional.
	`dns`	Endereço IP do servidor DNS do ponto de conexão externo. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • `AUTO` — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção `configurations`. Configuração opcional.
	`group`	O grupo a que o ponto de conexão externo pertence. Essa configuração é necessária se vários VDUs na função de rede física usarem o mesmo ponto de conexão externo.

Exemplo dessa seção

```
external_connections:
- name: LAN
 description: eth1
 ip: 192.168.2.0
 mask: 255.255.255.0
 gw: 192.168.0.1
 dns: 192.168.0.10
 group: lan-group
```

`internal_connections`

A seção `internal_connections` tem a seguinte estrutura:

Seção/configuração		Descrição
`- name`		Nome do ponto de conexão interno.
	`description`	Breve descrição do ponto de conexão interno.
	`ip`	Endereço IP do ponto de conexão interno. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • `AUTO` — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção `configurations`.
	`mask`	Máscara de sub-rede do ponto de conexão interno. Valores possíveis: • Valor no formato XXX.XXX.XXX.XXX, por exemplo: `255.255.255.0` A máscara de sub-rede é atribuída usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, a máscara de sub-rede não pode ser alterada. • AUTO — A máscara de sub-rede é atribuída automaticamente usando um servidor DHCP externo ou um script da seção `configurations`.
	`gw`	Endereço IP do gateway do ponto de conexão interno. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • `AUTO` — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção `configurations`. Configuração opcional.
	`dns`	Endereço IP do servidor DNS do ponto de conexão interno. Valores possíveis: • Valor no formato `XXX.XXX.XXX.XXX`, por exemplo: `192.168.110.126` O endereço IP é atribuído usando DHCP via reserva baseada em MAC de uma porta OpenStack. Nesse caso, o endereço IP não pode ser alterado. • `AUTO` — O endereço IP é atribuído automaticamente usando um servidor DHCP externo ou um script da seção `configurations`. Configuração opcional.
	`group`	O grupo a que o ponto de conexão interno pertence. Essa configuração é necessária se vários VDUs na função de rede física usarem o mesmo ponto de conexão interno.

Exemplo dessa seção

```
internal_connections:
- name: LAN
 description: eth3
 ip: 192.168.2.0
 mask: 255.255.255.0
 gw: 192.168.0.1
 dns: 192.168.0.10
 group: lan-group
```

`configurations`

A seção `configurations` tem a seguinte estrutura:

Seção/configuração		Descrição
- name		Nome da função.
	filename	Nome do arquivo do script ou do manual do Ansible. É necessário colocar o script no diretório /scripts do pacote de PNF.
	stage	O estágio de operação da função de rede física no qual o script é executado. Valores possíveis: • initialization para executar o script na implementação da função de rede física. • termination para executar o script na exclusão da função de rede física. • none para executar o script quando um valor for alterado na seção user_configurations na área de configurações da função de rede física na interface da Web do orquestrador.
	executor	Interpretador de scripts. Valores possíveis: • ansible • expect • /bin/sh • bin/bash • < caminho para o interpretador de script personalizado >, por exemplo /usr/bin/php
	authentication	Método de autenticação do VNFM na função de rede física para a execução de scripts. Valores possíveis: • key significa que o VNFM é autenticado na função de rede física usando uma chave gerada quando a função de rede física é implementada. É necessário usar um script para obter a chave, portanto, recomendamos não especificar esse valor para o primeiro script. • password significa que o VNFM é autenticado na função de rede física com um nome de usuário e senha da seção flavours → vdus.
	files_path	Caminho de arquivos para executar scripts usando SSH. É necessário criar um diretório no diretório /scripts do pacote de PNF e colocar os arquivos nele. Os arquivos são copiados para a VDU. Configuração opcional.
	timeout	O tempo de espera para a conclusão do script, em segundos. Se o script não for concluído dentro do tempo especificado, a execução será encerrada. O tempo limite começa no momento em que o script é executado. Especifique esse parâmetro caso tenha especificado um caminho para um executor de script personalizado para o parâmetro executor.

Exemplo dessa seção

```
configurations:
 - name: config
 filename: config.yml
 stage: initialization
 executor: ansible
 authentication: password
 files_path: SSH_scripts
 config_drive: true
 timeout: 15
```

flavours

A seção flavours tem a seguinte estrutura:

Seção/configuração		Descrição
- name		Nome da variação.
	description	Breve descrição da variação.
	position	Número sequencial da variação. A variação com a posição mais baixa tem o desempenho mais baixo.
	management	Parâmetros dos consoles de administração VDU.
	vdus	Configurações de VDU.

A seção management tem a seguinte estrutura:

Seção/configuração			Descrição
`ssh`			Configurações para gerenciar VDUs usando o console SSH.
	`- vdu_name`		Nome da VDU.
		`def_user`	Nome de usuário para estabelecer a sessão SSH.
		`authentication`	Método de autenticação do VNFM na função de rede física para a execução de scripts. Valores possíveis: • `key` significa que o VNFM é autenticado na função de rede física usando uma chave gerada quando a função de rede física é implementada. É necessário obter a chave usando um script da seção `configurations`. • `password` significa que o VNFM é autenticado na função de rede física com um nome de usuário e senha da seção `vdus`.
`web`			Configurações para gerenciar VDUs usando o console da Web.
	`- vdu_name`		Nome da VDU.
		`protocol`	Protocolo para conexão com o console da Web. Valores possíveis: • `http`. • `https`.
		`port`	Porta para conexão com o console da Web. Insira um valor no intervalo de 1 a 65.536. Por padrão, é especificado o número de porta 80.
		`path`	Caminho para o console da Web.
		`def_user`	Nome de usuário para autenticação no console da Web.
		`def_password`	Senha para autenticação no console da Web.

A seção `vdus` tem a seguinte estrutura:

Seção/configuração			Descrição
`- name`			Nome da VDU.
	`password_rules`		Requisitos de senha da VDU. Essa seção é opcional.
		`length`	Comprimento mínimo da senha.
		`use_upper_case`	Os usuários devem usar caracteres maiúsculos na senha. Valores possíveis: • `true` • `false`
		`use_lower_case`	Os usuários devem usar caracteres minúsculos na senha. Valores possíveis: • `true` • `false`
		`use_digits`	Os usuários devem usar numerais na senha. Valores possíveis: • `true` • `false`
		`specific_symbols`	Se os usuários devem usar caracteres especiais na senha, como: `@"!`
		`specific_symbols_min_usage`	Número mínimo de caracteres especiais que devem estar presentes na senha.
	`check_connection_mode`		Tipo de teste de disponibilidade da VDU executado durante a implementação. Por padrão, é executado um teste SSH. Valores possíveis: • `ssh` • `none` Configuração opcional.
	`zabbix_template`		Nome do modelo Zabbix para a VDU.
	`monitoring_type`		Tipo de monitoramento da função de rede física. Valores possíveis: • `agent` significa monitorar usando um agente Zabbix. • `snmp` significa monitorar usando o protocolo SNMP.
	`ssh_port`		Número da porta para estabelecer uma sessão SSH. Configuração opcional.
	`ssh_host_key_algorithm`		O algoritmo de chave do host usado. Valores possíveis: • `ssh-rsa`. • `ssh-ed25519`. Recomendamos usar esse algoritmo de chave de host pois ele é criptograficamente forte. Caso essa configuração não seja especificada, o algoritmo ssh-rsa é usado por padrão para compatibilidade com versões anteriores.

	`configurations`		Nomes de scripts da seção `configurations` a serem executados na VDU. Especifique uma lista de valores, por exemplo:
			`vdu_name:`
			`- config_1`
			`- config_2`

	`backups`		Nomes das tarefas de backup dos `backups` a serem usados na VDU. Especifique uma lista de valores, por exemplo:
			`vdu_name:`
			`- backup_1`
			`- backup_2`
			Essa seção é opcional.

	`def_user`		Nome de usuário para autenticar o VNFM na função de rede física. Configuração opcional.
	`def_password`		Senha para autenticar o VNFM na função de rede física. Configuração opcional.
	`password_authentication`		Autenticação de senha do VNFM na função de rede física. Valores possíveis: • `sim` • `Não` Configuração opcional.

Seção/configuração			Descrição
network_interfaces			Configurações da interface de rede
	- name		Nome da interface de rede.
		type	Tipo da interface de rede. Valores possíveis: • data é uma interface de rede para transferência de dados. • management é uma interface de rede de gerenciamento mapeada para uma porta de rede.
		description	Breve descrição da interface de rede.
		connection_point_ref	Nome do ponto de conexão externo da seção external_configurations para a interface de rede de gerenciamento.
auto_healing			Parâmetros de recuperação automática da VDU.
	triggers_set		Acionadores externos que iniciam a recuperação automática da VDU. Valores possíveis: • any para que qualquer acionador externo inicie a recuperação automática da VDU. • all para iniciar a recuperação automática da VDU se todos os acionadores externos especificados forem acionados. • < nome do acionador > para iniciar a recuperação automática da VDU quando o acionador externo especificado for acionado.
	triggers		Acionadores externos.
		- name	Nome do acionador externo. Valores possíveis: • unreachable • scale_up • scale_down
	action_set		Ação a ser executada quando um acionador externo é acionado.
		- type	Tipo de ação. Valores possíveis: • reboot para reiniciar a VDU. • script para executar o script especificado.
		configuration_name_ref	Nome do script da seção configurations executado quando um acionador externo é acionado. Esse parâmetro deve ser especificado caso script tenha sido selecionado como - type.

Exemplo dessa seção

```
vdus:
 - name: vgw
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 check_connection_mode: none
 zabbix_template: Template OS Linux
 monitoring_type: agent
 ssh_port: 22
 configurations:
 - config_1
 - config_2
 backups:
 - backup_config
 def_user: root
 def_password: p@ssw0rd
 password_authentication: yes
```

```
network_interfaces:
- name: eth
type: data
description: eth0
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
```

scaling

A seção `scaling` tem a seguinte estrutura:

Configuração	Descrição
`scale_up_status`	Dimensionamento vertical para uma variação com um número sequencial mais baixo. Valores possíveis: • `permit` • `deny`
`scale_down_status`	Dimensionamento vertical para uma variação com um número sequencial mais alto. Valores possíveis: • `permit` • `deny`

Exemplo dessa seção

```
scaling:
 scale_in_status: permit
 scale_out_status: permit
```

user_configurations

A seção `user_configurations` tem a seguinte estrutura:

Seção/configuração	Descrição
`tab`	Guias adicionadas à área de configurações da função de rede física.
`- name`	Nome da guia.

Seção/configuração			Descrição
	`variables`		Entradas da interface da Web do orquestrador que são exibidas na guia.
	`- name`		Nome da entrada da interface da Web do orquestrador.
		`description`	Breve descrição da entrada da interface da Web do orquestrador.
		`input_type`	Tipo de entrada da interface da Web do orquestrador. Valores possíveis: • `input` para adicionar um campo. • `dropdown` para adicionar uma lista suspensa.
		`default_value`	Valor padrão do campo. É possível especificar esse parâmetro caso `input` tenha sido especificado como `input_type`.
		`values`	As opções exibidas na lista suspensa. É possível especificar essa configuração caso `dropdown` tenha sido especificado como `input_type`.
		`- value`	O nome do valor.
		`is_default`	Valor padrão. Valores possíveis: • `true` • `false` Configuração opcional.
		`required`	Entrada obrigatória da interface da Web do orquestrador. Valores possíveis: • `true` • `false` Configuração opcional.
		`type`	Tipo de valor que pode ser especificado na entrada da interface da Web do orquestrador. Configuração opcional.
		`example`	Uma dica de ferramenta exibida quando o valor da entrada da interface da Web do orquestrador é alterado. Configuração opcional.

		`update_configuration_name`	Nomes de scripts da seção `configurations` executados quando o valor da entrada da interface da Web do orquestrador é alterado. Especifique uma lista de valores, por exemplo:
			`update_configuration_name:`
			`- config_1`
			`- config_2`

Exemplo dessa seção

```
user_configurations:
 tab:
 - name: GW
 variables:
 - name: "gw_ip"
 description: IP
 input_type: input
 required: true
 type: string
 default_value: 192.168.0.1
 example: 192.168.0.1
 - name: direction
 description: traffic direction
 input_type: dropdown
 required: true
 type: string
 values:
 - value: in
 is_default: true
```

```
- value: out
update_configuration_name:
- update_var
- change
```

backups

A seção backups tem a seguinte estrutura:

Seção/configuração			Descrição
- name			Nome da tarefa de backup.
	description		Breve descrição da tarefa de backup.
	backup		Parâmetros de backup.
		path	Caminho para o diretório da função de rede física onde os para backup estão localizados.
		interval	Intervalo de tempo em segundos para o backup.
		store_config	Número de cópias de backup a serem mantidas.
		backup_type	Tipo de backup.
		authentication	Método de autenticação do VNFM na função de rede física para a execução de scripts. Valores possíveis: • key significa que o VNFM é autenticado na função de rede física usando uma chave gerada quando a função de rede física é implementada. É necessário obter a chave usando um script da seção configurations. • password significa que o VNFM é autenticado na função de rede física com um nome de usuário e senha da seção flavours → vdus.
		configuration_name_ref	Nome do script da seção configurations a ser executado antes do backup.
	restore		Parâmetros de restauração de backup.
		path	Caminho para o diretório da função de rede física onde os arquivos restaurados são colocados.
		backup_type	Tipo de backup.
		authentication	Método de autenticação do VNFM na função de rede física para a execução de scripts. Valores possíveis: • key significa que o VNFM é autenticado na função de rede física usando uma chave gerada quando a função de rede física é implementada. É necessário obter a chave usando um script da seção configurations. • password significa que o VNFM é autenticado na função de rede física com um nome de usuário e senha da seção flavours → vdus.
		configuration_name_ref	Nome do script da seção configurations a ser executado após o início da restauração a partir do backup.

Exemplo dessa seção

```
backups:
 - name: backup_config
 description: backup/etc/config
 backup:
 path: /root/config.thz
 interval: 600
 store_configs: 10
 backup_type: vnfm_scp
 authentication: key
 configuration_name_ref: backup
 restore:
 path: /tmp/config.tgz
```

```
backup_type: vnfm_scp
authentication: password
configuration_name_ref: restore
```

Proteção de pacotes VNF e PNF contra substituição e modificação

Alguns arquivos de pacote de VNF e PNF são colocados no diretório local do contêiner Docker do orquestrador, e é possível protegê-los contra substituição e modificação. Quando os pacotes VNF e PNF são protegidos, o orquestrador automaticamente computa o hash SHA256 quando eles são carregados na interface da Web do orquestrador. Ao acessar arquivos no diretório local do contêiner Docker, o orquestrador compara seu hash SHA256 atual com o hash salvo anteriormente. Se os hashes SHA256 não forem correspondentes, o orquestrador impede que os usuários executem ações com a função de rede, como adicioná-la à topologia de um serviço de rede.

Para proteger os pacotes VNF e PNF contra substituição e modificação:

1. No menu, acesse a seção **Sistema**.

   Por padrão, é selecionada a guia **Monitoramento**, que exibe as configurações de conexão do servidor Zabbix.

2. Selecione a guia **Outro** e marque a caixa de seleção **Calcular soma de verificação SHA256 para arquivos de VNF/PNF armazenados**. Esta caixa de seleção é selecionada por padrão.

Os pacotes VNF e PNF são protegidos contra substituição e modificação.

Carregar um pacote de VNF ou PNF para a interface da Web do orquestrador

Para carregar um pacote de VNF ou PNF para a interface da Web do orquestrador:

1. No menu, acesse a seção **Catálogo**.

   A página de gerenciamento do serviço de rede é exibida.

2. Na parte superior da página, clique em **+ VNF** ou **+ PNF**.

3. Na janela aberta, selecione o pacote de VNF ou PNF.

4. Para verificar a integridade do pacote de VNF ou PNF, insira o hash SHA256 do pacote no campo **Hash sum SHA256**. O comprimento máximo do hash é de 64 caracteres.

5. Clique em **Salvar**.

O pacote de VNF ou PNF é carregado na interface da Web do orquestrador. O VNF ou PNF é exibido no painel **Catálogo**. Caso tenha inserido um hash SHA256 de um pacote de VNF ou PNF, o orquestrador compara o hash inserido com o hash SHA256 real. Se os hashes SHA256 não forem correspondentes, o pacote de VNF ou PNF não será carregado.

Especificar uma breve descrição para um serviço de rede compartilhado

É possível especificar uma breve descrição do serviço de rede compartilhado.

1. Acesse a topologia de uma das seguintes formas:
   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.
2. Na ferramenta de design gráfico, clique no serviço de rede compartilhado para o qual deseja especificar uma breve descrição.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Configurações**, que exibe uma breve descrição do serviço de rede compartilhado.
3. No campo **Descrição**, insira uma breve descrição do serviço de rede compartilhado.
4. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do serviço de rede compartilhado.

Gerenciar funções de rede virtual

Para gerenciar uma função de rede virtual, execute uma das seguintes ações:

- No portal do administrador, vá para a seção **Catálogo** e, no painel **Catálogo**, clique na função de rede virtual.
- Ao criar ou editar um modelo de serviço de rede na topologia, clique na função de rede virtual.
- Ao criar ou editar um serviço de rede na topologia, clique na função de rede virtual.

É possível gerenciar as configurações de funções de rede virtual nas seguintes guias:

- **Tipos** contém variações da função de rede virtual.
- **Pontos de conexão** contém pontos de conexão externos da função de rede virtual.
- **Configurações de VNF** contém configurações básicas da função de rede virtual.
- **Posicionamento** contém configurações de posicionamento da função de rede virtual. É possível colocar uma função de rede virtual em um data center ou um dispositivo uCPE. Essa guia é exibida caso a função de rede virtual tenha sido clicada ao criar ou editar um serviço de rede.

As seguintes guias são exibidas caso a função de rede virtual tenha sido clicada na topologia de um serviço de rede implementado:

- **Gerenciamento de VDU** é uma tabela de VDUs que fazem parte da função de rede virtual. As informações sobre VDUs são exibidas nas seguintes colunas da tabela:
  - **Nome** é o nome da VDU.
  - **Nome da instância** é o ID da instância da VDU.
  - **IP de gestão** é o endereço IP que a sub-rede de gerenciamento atribuiu à VDU.
  - **vCPU** é o número de núcleos de CPU virtuais atribuídos à VDU.
  - **RAM** é a quantidade de RAM, em megabytes, atribuída à VDU.
  - **Disco** é o espaço em disco, em gigabytes, atribuído à VDU.
  - **Status** é o status da VDU:
    - **ACTIVE** significa que a VDU está funcionando normalmente.
    - **ERROR** significa que a VDU encontrou um erro.
    - **HARD_REBOOT** significa que uma reinicialização forçada da VDU está em andamento.
    - **PAUSED** significa que a VDU está pausada.
    - **REBOOT** significa que uma reinicialização suave da VDU está em andamento.
    - **SHUTOFF** significa que a VDU foi interrompida.
    - **SUSPENDED** significa que a VDU está suspensa.
- **Monitoramento** contém resultados de monitoramento da função de rede virtual.
- **Problemas** contém problemas que ocorreram durante a operação da função de rede virtual. Em caso de problemas, um ponto de exclamação vermelho é exibido ao lado da guia.

Além disso, as guias especificadas na seção `user_configurations` do descritor de VNF podem ser exibidas.

Selecionar a variação de uma função de rede virtual

É possível especificar variações na seção `variações` do descritor de VNF.

Para selecionar a variação de uma função de rede virtual:

1. Acesse a topologia de uma das seguintes formas:
   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique na função de rede virtual para a qual deseja selecionar uma variação.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

3. Selecione uma variação para a função de rede virtual.

4. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da função de rede virtual.

Configurar pontos de conexão externos de uma função de rede virtual

É possível especificar pontos de conexão externos de uma função de rede virtual na seção `external_connections` do descritor de VNF.

Para configurar pontos de conexão externos da função de rede virtual:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique na função de rede virtual cujos pontos de conexão externos deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

3. Selecione a guia **Pontos de conexão**.

   Isso exibe os pontos de conexão externos da função de rede virtual.

4. Na lista suspensa **Tipo**, selecione como deseja atribuir um prefixo IPv4 ao ponto de conexão externo:

   - **Reserva de DHCP** para usar DHCP para atribuir um prefixo IPv4 ao ponto de montagem externo. Ao selecionar essa opção, faça o seguinte:

     a. No campo **Endereço IP**, insira o endereço IPv4 que o DHCP atribui ao ponto de conexão externo.

     b. No campo **Máscara**, insira a máscara de sub-rede que o DHCP atribui ao ponto de conexão externo.

   - **AUTO** para atribuir um prefixo IPv4 ao ponto de conexão externo automaticamente. Essa é a configuração padrão.

5. No campo **Descrição**, insira uma breve descrição do ponto de conexão externo.

6. Para definir o ponto de conexão como porta de tronco, marque a caixa de seleção **Tronco**. Esta caixa de seleção está desmarcada por padrão.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da função de rede virtual.

Configurações básicas de uma função de rede virtual

Para editar as configurações básicas da função de rede virtual:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique na função de rede virtual cujas configurações básicas deseja definir.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

3. Selecione a guia **Configurações de VNF**.

   As configurações básicas da função de rede virtual são exibidas.

4. No campo **Nome**, insira o nome da função de rede virtual.

5. No campo **Descrição**, insira uma breve descrição da função de rede virtual.

6. No campo **Ordem**, insira o número de sequência para a implementação da função de rede virtual na plataforma de nuvem OpenStack. Ao implementar um serviço de rede, a função de rede virtual com o número mais baixo é a primeira a ser implementada. Se nenhuma das funções de rede virtual adicionadas à topologia do serviço de rede tiver um número de sequência especificado, todas as funções de rede virtual serão implementadas simultaneamente.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da função de rede virtual.

Hospedar a função de rede virtual em um data center e em um dispositivo uCPE

Para colocar uma função de rede virtual em um data center ou um dispositivo uCPE.

1. Navegue até a topologia começando a criar ou editar um serviço de rede.

2. Clique na função de rede virtual que deseja colocar em um data center ou em um dispositivo uCPE.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

3. Selecione a guia **Posicionamento**.

   As configurações de posicionamento da função de rede virtual são exibidas.

4. Na lista **Selecione o tipo de posicionamento**, selecione um dos seguintes valores:

   - **Data center** para colocar a função de rede virtual no data center especificado. Ao selecionar essa opção, faça o seguinte:

     a. No campo **Data center**, insira o nome do data center criado. Conforme você digita o nome, é solicitado que selecione um data center em uma lista suspensa.

     b. No campo **VIM**, insira o nome do VIM implementado para a função de rede virtual. Conforme você digita o nome, é solicitado que selecione um VIM em uma lista suspensa.

   - **uCPE** para colocar a função de rede virtual no dispositivo uCPE especificado. Ao selecionar esta opção, no campo **uCPE**, insira o nome do dispositivo uCPE. Conforme você digita o nome, é solicitado que selecione um dispositivo uCPE em uma lista suspensa.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da função de rede virtual.

Interromper ou iniciar uma função de rede virtual ou uma VDU que faz parte dela

É possível interromper uma função de rede virtual ou uma VDU que faz parte dela para liberar os recursos computacionais da plataforma de nuvem OpenStack.

Ao iniciar uma função de rede virtual ou VDU, ela volta a consumir recursos computacionais. Isso reinicia os processos em execução na função de rede virtual ou VDU.

Para interromper ou iniciar uma função de rede virtual ou uma VDU que faz parte dela:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Para interromper ou iniciar uma função de rede virtual, na parte superior da área de configurações, clique em **Gerenciamento** → **Energia** → **Interromper VNF** ou **Iniciar VNF**.

5. Para interromper ou iniciar uma VDU que faz parte da função de rede virtual:

   a. Selecione a guia **Gerenciamento de VDU**.

      Uma tabela de VDUs é exibida.

   b. Clique em **Gerenciamento** → **Energia** → **Interromper VDU** ou **Iniciar VDU** ao lado da VDU que deseja interromper ou iniciar.

6. Na janela de confirmação, clique em **Aplicar**.

A função de rede virtual ou sua VDU é interrompida ou iniciada.

Pausar ou retomar uma função de rede virtual ou uma VDU que faz parte dela

É possível pausar uma função de rede virtual ou uma VDU que faz parte dela para interromper processos em execução. No entanto, a função de rede virtual ou VDU continua a consumir os recursos computacionais da plataforma de nuvem OpenStack. Quando uma função de rede virtual ou uma VDU é retomada, os processos em execução são retomados.

Para pausar ou retomar uma função de rede virtual ou uma VDU que faz parte dela:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Pause ou retome a função de rede virtual ou uma VDU que faz parte dela:

   - Para pausar ou retomar uma função de rede virtual, na parte superior da área de configurações, clique em **Gerenciamento** → **Energia** → **Pausar VNF** ou **Retomar VNF**.

   - Para pausar ou retomar uma VDU que faz parte da função de rede virtual:

     1. Selecione a guia **Gerenciamento de VDU**.

        Uma tabela de VDUs é exibida.

     2. Clique em **Gerenciamento** → **Energia** → **Pausar VDU** ou **Retomar VDU**.

5. Na janela de confirmação, clique em **Aplicar**.

A função de rede virtual ou sua VDU é pausada ou retomada.

Suspender ou cancelar a suspensão de uma função de rede virtual ou de uma VDU que faz parte dela

É possível suspender uma função de rede virtual ou uma VDU que faz parte dela para liberar os recursos computacionais da plataforma de nuvem OpenStack. Isso salva o estado da função de rede virtual ou VDU no disco da plataforma de nuvem OpenStack. Ao cancelar a suspensão da função de rede virtual ou VDU, ela volta a consumir recursos computacionais. Os processos em execução em uma função de rede virtual ou VDU são retomados a partir do ponto em que seu estado foi salvo.

Para suspender ou cancelar a suspensão de uma função de rede virtual ou de sua VDU:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Suspenda ou cancele a suspensão de uma função de rede virtual ou de sua VDU:

   - Para suspender ou cancelar a suspensão de uma função de rede virtual, na parte superior da área de configurações, clique em **Gerenciamento** → **Energia** → **Suspender VNF** ou**Retomar VNF suspensa**.

   - Para suspender ou cancelar a suspensão de uma VDU que faz parte da função de rede virtual:

     1. Selecione a guia **Gerenciamento de VDU**.

        Uma tabela de VDUs é exibida.

     2. Clique em **Gerenciamento** → **Energia** → **Suspender VDU** ou **Retomar VDU suspensa** ao lado da VDU que deseja suspender ou cancelar a suspensão.

5. Na janela de confirmação, clique em **Aplicar**.

A função de rede virtual ou sua VDU é suspensa ou tem sua suspensão cancelada.

Reinicialização suave de uma função de rede virtual ou de uma VDU que faz parte dela

Quando é executada uma reinicialização suave de uma função de rede virtual, todas as VDUs ativas nela são reiniciadas. Para executar a reinicialização suave de uma função de rede virtual, pelo menos uma VDU nela não pode estar suspensa.

Para executar a reinicialização suave de uma função de rede virtual ou de uma VDU que faz parte dela:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Execute uma reinicialização suave de uma função de rede virtual ou de sua VDU:

   - Para executar uma reinicialização suave da função de rede virtual, na parte superior da área de configurações, clique em **Gerenciamento** → **Energia** → **Reinicialização suave da VNF**.

   - Para executar uma reinicialização suave de uma VDU que faça parte da função de rede virtual:

     1. Selecione a guia **Gerenciamento de VDU**.

        Uma tabela de VDUs é exibida.

     2. Clique em **Gerenciamento** → **Energia** → **Reinicialização suave da VDU** ao lado da VDU na qual deseja executar a reinicialização suave.

5. Na janela de confirmação, clique em **Aplicar**.

É executada a reinicialização suave da função de rede virtual ou de sua VDU.

Reinicialização forçada de uma função de rede virtual ou de uma VDU que faz parte dela

A reinicialização forçada simula o ato de desligar e religar a energia. Recomendamos executar uma reinicialização forçada somente se a reinicialização suave não funcionar.

Para executar a reinicialização forçada de uma função de rede virtual ou de uma VDU que faz parte dela:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Para executar a reinicialização forçada de uma função de rede virtual ou de sua VDU:

   - Para executar a reinicialização forçada da função de rede virtual, na parte superior da área de configurações, clique em **Gerenciamento** → **Energia** → **Reinicialização forçada da VNF**.

   - Para executar a reinicialização forçada de uma VDU que faz parte da função de rede virtual:

     1. Selecione a guia **Gerenciamento de VDU**.

        Uma tabela de VDUs é exibida.

     2. Clique em **Gerenciamento** → **Energia** → **Reinicialização forçada da VDU** ao lado da VDU na qual deseja executar a reinicialização forçada.

5. Na janela de confirmação, clique em **Aplicar**.

É executada a reinicialização forçada da VNF ou de sua VDU.

Reimplementar uma função de rede virtual ou uma VDU que faz parte dela

A reimplantação de uma função de rede virtual ou de uma VDU que faz parte dela pode resultar em interrupções de curto prazo ou perda temporária de função. Ao planejar e coordenar atividades de reimplementação, recomendamos considerar as circunstâncias da organização para minimizar as interrupções.

Para reimplementar uma função de rede virtual ou uma VDU que faz parte dela:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Para reimplementar uma função de rede virtual ou sua VDU:

   - Para reimplementar a função de rede virtual, na parte superior da área de configurações, clique em **Gerenciamento → Reimplementar VNF**.

   - Para reimplementar uma VDU que faz parte da função de rede virtual:

     1. Selecione a guia **Gerenciamento de VDU**.

        Uma tabela de VDUs é exibida.

     2. Clique em **Gerenciamento → Reimplementar VDU** ao lado da VDU que deseja reimplementar.

5. Na janela de confirmação, clique em **Confirmar**.

A reimplementação da função de rede virtual ou de sua VDU é iniciada, o que pode levar vários minutos. Para interromper a implementação, clique em **Interromper implementação**.

Recuperação automática de uma função de rede virtual ou de uma VDU que faz parte dela

É possível executar a recuperação automática de uma função de rede virtual ou uma VDU que faz parte dela, mesmo se a recuperação automática tiver sido desativada para o serviço de rede em cuja topologia a função de rede virtual foi adicionada.

Para executar a recuperação automática de uma função de rede virtual ou de uma VDU que faz parte dela:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Execute a recuperação automática da função de rede virtual ou de sua VDU.

   - Para executar a recuperação automática da função de rede virtual, na parte superior da área de configurações, clique em **Gerenciamento** → **Recuperar VNF**.
   - Para executar a recuperação automática de uma VDU que faz parte da função de rede virtual:

     1. Selecione a guia **Gerenciamento de VDU**.

        Uma tabela de VDUs é exibida.

     2. Clique em **Gerenciamento** → **Recuperar VDU** ao lado da VDU na qual deseja executar a recuperação automática.

5. Na janela de confirmação, clique em **Aplicar**.

A recuperação automática de uma função de rede virtual ou de uma VDU que faz parte dela é iniciada.

Gerenciar instantâneos de VDU

Para visualizar a tabela de instantâneos de VDU, clique na função de rede virtual na topologia do serviço de rede implementado, selecione a guia **Gerenciamento de VDU** e clique em **Gerenciamento** → **Instantâneo** ao lado do VDU.

As informações sobre os instantâneos de VDU são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do instantâneo de VDU.
- **Criado em** é a data e hora em que o instantâneo de VDU foi criado.
- **Tamanho** é o tamanho do instantâneo de VDU em bytes.
- **Descrição** é uma breve descrição do instantâneo de VDU.
- **Gerenciamento** contém ações que podem ser executadas no instantâneo de VDU.

Criar um instantâneo de VDU

Não recomendamos armazenar instantâneos por muito tempo, pois existência deles reduz o desempenho do VDU.

Para gerar um instantâneo de VDU:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual que inclui o VDU.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Selecione a guia **Gerenciamento de VDU**.

   Uma tabela de VDUs é exibida.

5. Clique em **Energia** → **Instantâneo** ao lado do VDU da qual deseja criar um instantâneo.

   Isso abre uma janela com a tabela de instantâneos de VDU.

6. No campo **Nome**, insira um nome para o instantâneo do VDU.

7. No campo **Descrição**, insira uma breve descrição do instantâneo do VDU.

8. Clique em **Criar**.

Um instantâneo do VDU é criado e exibido na tabela.

Restaurar as configurações de um VDU usando um instantâneo

Para restaurar as configurações do VDU usando um instantâneo:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual que inclui o VDU.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ⤢. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Selecione a guia **Gerenciamento de VDU**.

   Uma tabela de VDUs é exibida.

5. Clique em **Energia** → **Instantâneo** ao lado do VDU cujas configurações deseja restaurar usando o instantâneo.

   Isso abre uma janela com a tabela de instantâneos de VDU.

6. Clique em **Gerenciamento** → **Reverter** ao lado do instantâneo que deseja usar para restaurar as configurações do VDU.

7. Na janela de confirmação, clique em **Reverter**.

As configurações da VDU são restauradas de acordo com o instantâneo.

Editar um instantâneo de VDU

Para editar um instantâneo de VDU:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual que inclui o VDU.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Selecione a guia **Gerenciamento de VDU**.

   Uma tabela de VDUs é exibida.

5. Clique em **Energia** → **Instantâneo** ao lado do VDU cujo instantâneo deseja editar.

   Isso abre uma janela com a tabela de instantâneos de VDU.

6. Clique em **Gerenciamento** → **Editar** ao lado do instantâneo de VDU que deseja editar.

7. Na janela aberta, se necessário, edite o nome e/ou a descrição do instantâneo do VDU.

8. Clique em **Salvar**.

O instantâneo do VDU é modificado e atualizado na tabela.

Excluir um instantâneo de VDU

Os instantâneos de VDU excluídos não podem ser restaurados.

Para excluir um instantâneo de VDU:

1. No portal de autoatendimento, acesse a seção **Catálogo** do menu.

   A página de gerenciamento do serviço de rede é exibida.

2. No painel **Serviços de rede**, clique no serviço de rede implementado à cuja topologia a função de rede virtual foi adicionada.

   A topologia é exibida.

3. Clique na função de rede virtual que inclui o VDU.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

4. Selecione a guia **Gerenciamento de VDU**.

   Uma tabela de VDUs é exibida.

5. Clique em **Energia** → **Instantâneo** ao lado do VDU cujo instantâneo deseja editar.

   Isso abre uma janela com a tabela de instantâneos de VDU.

6. Clique em **Gerenciamento** → **Excluir** ao lado do instantâneo de VDU que deseja excluir.

7. Na janela de confirmação, clique em **Excluir**.

O instantâneo de VDU é excluído e não é mais exibido na tabela.

Gerenciar funções de rede física

Para gerenciar uma função de rede física, execute uma das seguintes ações:

- No portal do administrador, vá para a seção **Catálogo** e, no painel **Catálogo**, clique na função de rede física.
- Ao criar ou editar um modelo de serviço de rede na topologia, clique na função de rede física.
- Ao criar ou editar um serviço de rede na topologia, clique na função de rede física.

É possível gerenciar as configurações de funções de rede física nas seguintes guias:

- **Tipos** contém variações da função de rede física.
- **Configurações de VNF** contém configurações básicas da função de rede física.

As seguintes guias são exibidas caso a função de rede física tenha sido clicada na topologia de um serviço de rede implementado:

- **Monitoramento** contém resultados de monitoramento da função de rede física.
- **Problemas** contém problemas que ocorreram durante a operação da função de rede física. Em caso de problemas, um ponto de exclamação vermelho é exibido ao lado da guia.

Além disso, as guias especificadas na seção `user_configurations` do descritor de PNF podem ser exibidas.

Selecionar a variação de uma função de rede física

É possível especificar variações na seção `variações` do descritor de PNF.

Para selecionar a variação de uma função de rede física:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique na função de rede física para a qual deseje selecionar uma variação.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

3. Selecione uma variação para a função de rede física.

4. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da função de rede física.

Configurações básicas de uma função de rede física

Para editar as configurações básicas da função de rede física:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique na função de rede física cujas configurações básicas deseja definir.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Tipos**, que exibe as variações.

3. Selecione a guia **Configurações da PNF**.

   As configurações básicas da função de rede física são exibidas.

4. No campo **Nome**, insira o nome da função de rede física.

5. No campo **Descrição**, insira uma breve descrição da função de rede física.

6. No campo **Ordem**, insira o número de sequência para implementação da função de rede física. Ao implementar um serviço de rede, a função de rede física com o número mais baixo é a primeira a ser implementada. Se nenhuma das funções de rede física adicionadas à topologia tiver um número de sequência especificado, todas as funções de rede física serão implementadas simultaneamente.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da função de rede física.

Configurar um serviço P2P

Para configurar um serviço P2P:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique no serviço P2P que deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

3. No campo **Nome**, insira o nome do serviço P2P.

4. Se necessário, no campo **Descrição**, insira uma breve descrição do serviço P2P.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do serviço P2P.

Configurar um serviço P2M

Para configurar um serviço P2M:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique no serviço P2M que deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

3. No campo **Nome**, insira o nome do serviço P2M.

4. Se necessário, no campo **Descrição**, insira uma breve descrição do serviço P2M.

5. No campo **Pontos de conexão**, insira o número máximo de pontos de conexão de serviço P2M. Intervalo de valores: 2 a 9999. Caso não seja especificado um valor para essa configuração, o número de pontos de conexão será ilimitado.

6. Na lista suspensa **Modo**, selecione se o serviço P2M usa uma DFI (Interface de encaminhamento padrão), para a qual o tráfego unicast desconhecido é enviado:

   - **Clássico** caso não deseje usar uma DFI. Essa é a configuração padrão.
   - **DFI com FIB na raiz e folhas** para usar uma DFI na interface de serviço com a função raiz.
   - **DFI com FIB na folha** para usar uma DFI na interface de serviço com a função raiz. É necessário criar interfaces de serviço com a função folha no mesmo dispositivo CPE. As interfaces de serviço de backup com a função folha devem ser criadas no mesmo dispositivo CPE, que deve ser diferente do dispositivo CPE no qual as interfaces de serviço principais foram criadas.

7. No campo **Idade do MAC (s)**, insira o tempo (em segundos) durante o qual as entradas são mantidas na tabela MAC do controlador. Intervalo de valores: 10 a 65.535. O valor padrão é `300`.

8. Na lista suspensa **Modo de aprendizado MAC**, selecione a ação que deseja aplicar a uma série de quadros quando o primeiro for enviado ao controlador para saber o endereço MAC de origem:

   - **Aprender e inundar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros será enviada para todas as interfaces de serviço adicionadas ao serviço P2M, exceto para a interface de serviço na qual a série de quadros chegou originalmente. Essa é a configuração padrão.

   - **Aprender e descartar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros é descartada.

   Se o endereço MAC de destino estiver presente na tabela MAC, a série de quadros é enviada para a interface de serviço de destino.

9. No campo **Tamanho da tabela MAC**, insira o número máximo de entradas na tabela MAC no controlador. Intervalo de valores: 0 a 65.535. `0` significa que o número de entradas não é limitado. O valor padrão é `100`.

10. Na lista suspensa **Sobrecarga da tabela MAC**, selecione a política de processamento de novos endereços MAC quando a tabela MAC do controlador está cheia:

    - **Inundação** significa que o tráfego com endereços MAC de destino que não foram aprendidos é transmitido como tráfego BUM (broadcast, unknown-unicast e multicast). Essa é a configuração padrão.

    - **Descartar** significa que o tráfego com endereços MAC de destino que não foram aprendidos é descartado.

11. Para configurar a atribuição de endereços IP às funções de rede virtual usando DHCP:

    a. Na lista suspensa **DHCP do OpenStack**, selecione **Ativado**. O valor padrão é **Desativar**.

    b. No campo **CIDR**, insira o prefixo IPv4 da sub-rede OpenStack que atribui endereços IP às funções de rede virtual.

    c. Caso deseje que a sub-rede OpenStack atribua um gateway específico às funções de rede virtual, insira o endereço IPv4 do gateway no campo **Gateway**.

    d. Especifique o intervalo de endereços IP do qual a sub-rede OpenStack atribui endereços IP às funções de rede virtual: para isso, em **Pools**, clique em **+ Pool** e insira os valores inicial e final do intervalo de endereços IP.

       O intervalo de endereços IP é especificado e exibido na seção **Pools**. É possível especificar diversos intervalos de endereços IP ou excluir intervalos de endereços IP. Para excluir um intervalo de endereços IP, clique em **Excluir** ao lado dele.

    e. Especifique o servidor DNS que a sub-rede OpenStack atribui às funções de rede virtual. Para isso, em **DNS**, clique em **+ DNS** e insira o endereço IPv4 do servidor DNS.

       O servidor DNS é especificado e exibido na seção **DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique em **Excluir** ao lado dele.

12. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do serviço P2M.

Configurar um serviço M2M

Para configurar um serviço M2M:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.

   - Comece a criar ou editar um serviço de rede.

2. Clique no serviço M2M que deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

3. No campo **Nome**, insira o nome do serviço M2M.

4. Se necessário, no campo **Descrição**, insira uma breve descrição do serviço M2M.

5. No campo **Pontos de conexão**, insira o número máximo de pontos de conexão de serviço M2M. Intervalo de valores: 2 a 9999. Caso não seja especificado um valor para essa configuração, o número de pontos de conexão será ilimitado.

6. No campo **Idade do MAC (s)**, insira o tempo (em segundos) durante o qual as entradas são mantidas na tabela MAC do controlador. Intervalo de valores: 10 a 65.535. O valor padrão é `300`.

7. Na lista suspensa **Modo de aprendizado MAC**, selecione a ação que deseja aplicar a uma série de quadros quando o primeiro for enviado ao controlador para saber o endereço MAC de origem:

   - **Aprender e inundar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros será enviada para todas as interfaces de serviço adicionadas ao serviço P2M, exceto para a interface de serviço na qual a série de quadros chegou originalmente. Essa é a configuração padrão.

   - **Aprender e descartar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros é descartada.

   Se o endereço MAC de destino estiver presente na tabela MAC, a série de quadros é enviada para a interface de serviço de destino.

8. No campo **Tamanho da tabela MAC**, insira o número máximo de entradas na tabela MAC no controlador. Intervalo de valores: 0 a 65.535. `0` significa que o número de entradas não é limitado. O valor padrão é `100`.

9. Na lista suspensa **Sobrecarga da tabela MAC**, selecione a política de processamento de novos endereços MAC quando a tabela MAC do controlador está cheia:

   - **Inundação** significa que o tráfego com endereços MAC de destino que não foram aprendidos é transmitido como tráfego BUM (broadcast, unknown-unicast e multicast). Essa é a configuração padrão.

   - **Descartar** significa que o tráfego com endereços MAC de destino que não foram aprendidos é descartado.

10. Para configurar a atribuição de endereços IP às funções de rede virtual usando DHCP:

    a. Na lista suspensa **DHCP do OpenStack**, selecione **Ativado**. O valor padrão é **Desativar**.

    b. No campo **CIDR**, insira o prefixo IPv4 da sub-rede OpenStack que atribui endereços IP às funções de rede virtual.

    c. Caso deseje que a sub-rede OpenStack atribua um gateway específico às funções de rede virtual, insira o endereço IPv4 do gateway no campo **Gateway**.

    d. Especifique o intervalo de endereços IP do qual a sub-rede OpenStack atribui endereços IP às funções de rede virtual: para isso, em **Pools**, clique em **+ Pool** e insira os valores inicial e final do intervalo de endereços IP.

    O intervalo de endereços IP é especificado e exibido na seção **Pools**. É possível especificar diversos intervalos de endereços IP ou excluir intervalos de endereços IP. Para excluir um intervalo de endereços IP, clique em **Excluir** ao lado dele.

    e. Especifique o servidor DNS que a sub-rede OpenStack atribui às funções de rede virtual. Para isso, em **DNS**, clique em **+ DNS** e insira o endereço IPv4 do servidor DNS.

    O servidor DNS é especificado e exibido na seção **DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique em **Excluir** ao lado dele.

11. Para usar um serviço M2M para criar um serviço de rede compartilhado, marque a caixa de seleção **Compartilhar serviço de rede**. Esta caixa de seleção está desmarcada por padrão.

12. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do serviço M2M.

Configurar uma rede compartilhada (OS 2 SHARED)

Para configurar uma rede compartilhada na topologia:

1. Acesse a topologia de uma das seguintes formas:

    - Comece a criar ou editar um modelo de serviço de rede.
    - Comece a criar ou editar um serviço de rede.

2. Clique na rede compartilhada que deseja configurar.

    A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

3. No campo **Nome**, insira o nome da rede compartilhada.

4. Se necessário, no campo **Descrição**, insira uma breve descrição da rede compartilhada.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da rede compartilhada.

Configurar um roteador virtual (OS vRouter)

Para configurar um roteador virtual:

1. Acesse a topologia de uma das seguintes formas:
   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.
2. Clique no roteador virtual que deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.
3. No campo **Nome**, insira o nome do roteador virtual.
4. Se necessário, no campo **Descrição**, insira uma breve descrição do roteador virtual.
5. Para definir o valor 'up' para o estado operacional do roteador virtual, marque a caixa de seleção **Estado administrativo**. Esta caixa de seleção está desmarcada por padrão.
6. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do roteador virtual.

Configurar uma VLAN

Para configurar uma VLAN:

1. Acesse a topologia de uma das seguintes formas:
   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.
2. Clique na VLAN que deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.
3. No campo **Nome**, insira o nome da VLAN.
4. Se necessário, no campo **Descrição**, insira uma breve descrição da VLAN.
5. Para configurar a atribuição de endereços IP às funções de rede virtual usando DHCP:
   a. Na lista suspensa **DHCP do OpenStack**, selecione **Ativado**. O valor padrão é **Desativar**.
   b. No campo **CIDR**, insira o prefixo IPv4 da sub-rede OpenStack que atribui endereços IP às funções de rede virtual.

c. Caso deseje que a sub-rede OpenStack atribua um gateway específico às funções de rede virtual, insira o endereço IPv4 do gateway no campo **Gateway**.

d. Especifique o intervalo de endereços IP do qual a sub-rede OpenStack atribui endereços IP às funções de rede virtual: para isso, em **Pools**, clique em **+ Pool** e insira os valores inicial e final do intervalo de endereços IP.

   O intervalo de endereços IP é especificado e exibido na seção **Pools**. É possível especificar diversos intervalos de endereços IP ou excluir intervalos de endereços IP. Para excluir um intervalo de endereços IP, clique em **Excluir** ao lado dele.

e. Especifique o servidor DNS que a sub-rede OpenStack atribui às funções de rede virtual. Para isso, em **DNS**, clique em **+ DNS** e insira o endereço IPv4 do servidor DNS.

   O servidor DNS é especificado e exibido na seção **DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique em **Excluir** ao lado dele.

6. Para usar a VLAN para criar um serviço de rede compartilhado, marque a caixa de seleção **Compartilhar rede**. Esta caixa de seleção está desmarcada por padrão.

7. Para atribuir uma tag VLAN às funções de rede virtual, no campo **ID de segmentação**, insira a tag VLAN.

8. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da VLAN.

Configurar uma VXLAN

Para configurar uma VXLAN:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique na VXLAN que deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

3. No campo **Nome**, insira o nome da VXLAN.

4. Se necessário, no campo **Descrição**, insira uma breve descrição da VXLAN.

5. Para configurar a atribuição de endereços IP às funções de rede virtual usando DHCP:

   a. Na lista suspensa **DHCP do OpenStack**, selecione **Ativado**. O valor padrão é **Desativar**.

   b. No campo **CIDR**, insira o prefixo IPv4 da sub-rede OpenStack que atribui endereços IP às funções de rede virtual.

   c. Caso deseje que a sub-rede OpenStack atribua um gateway específico às funções de rede virtual, insira o endereço IPv4 do gateway no campo **Gateway**.

d. Especifique o intervalo de endereços IP do qual a sub-rede OpenStack atribui endereços IP às funções de rede virtual: para isso, em **Pools**, clique em **+ Pool** e insira os valores inicial e final do intervalo de endereços IP.

   O intervalo de endereços IP é especificado e exibido na seção **Pools**. É possível especificar diversos intervalos de endereços IP ou excluir intervalos de endereços IP. Para excluir um intervalo de endereços IP, clique em **Excluir** ao lado dele.

e. Especifique o servidor DNS que a sub-rede OpenStack atribui às funções de rede virtual. Para isso, em **DNS**, clique em **+ DNS** e insira o endereço IPv4 do servidor DNS.

   O servidor DNS é especificado e exibido na seção **DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique em **Excluir** ao lado dele.

6. Para usar a VXLAN para criar um serviço de rede compartilhado, marque a caixa de seleção **Compartilhar rede**. Esta caixa de seleção está desmarcada por padrão.

7. Para atribuir uma tag VXLAN às funções de rede virtual, no campo **ID de segmentação**, insira a tag VXLAN.

8. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da VXLAN.

Configurar uma rede plana

Para configurar uma rede plana:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique na rede plana que deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

3. No campo **Nome**, insira o nome da rede plana.

4. Se necessário, no campo **Descrição**, insira uma breve descrição da rede plana.

5. Para configurar a atribuição de endereços IP às funções de rede virtual usando DHCP:

   a. Na lista suspensa **DHCP do OpenStack**, selecione **Ativado**. O valor padrão é **Desativar**.

   b. No campo **CIDR**, insira o prefixo IPv4 da sub-rede OpenStack que atribui endereços IP às funções de rede virtual.

   c. Caso deseje que a sub-rede OpenStack atribua um gateway específico às funções de rede virtual, insira o endereço IPv4 do gateway no campo **Gateway**.

d. Especifique o intervalo de endereços IP do qual a sub-rede OpenStack atribui endereços IP às funções de rede virtual: para isso, em **Pools**, clique em **+ Pool** e insira os valores inicial e final do intervalo de endereços IP.

   O intervalo de endereços IP é especificado e exibido na seção **Pools**. É possível especificar diversos intervalos de endereços IP ou excluir intervalos de endereços IP. Para excluir um intervalo de endereços IP, clique em **Excluir** ao lado dele.

e. Especifique o servidor DNS que a sub-rede OpenStack atribui às funções de rede virtual. Para isso, em **DNS**, clique em **+ DNS** e insira o endereço IPv4 do servidor DNS.

   O servidor DNS é especificado e exibido na seção **DNS**. É possível especificar vários servidores DNS ou excluir servidores DNS. Para excluir um servidor DNS, clique em **Excluir** ao lado dele.

6. Para usar a rede plana para criar um serviço de rede compartilhado, marque a caixa de seleção **Compartilhar rede**. Esta caixa de seleção está desmarcada por padrão.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da rede plana.

Configurar uma UNI

Para configurar uma UNI:

1. Acesse a topologia de uma das seguintes formas:

   - Comece a criar ou editar um modelo de serviço de rede.
   - Comece a criar ou editar um serviço de rede.

2. Clique na UNI que deseja configurar.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗.

3. No campo **Nome**, insira o nome da UNI.

4. Se necessário, no campo **Descrição**, insira uma breve descrição da UNI.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações da UNI.

Monitorar componentes da solução

Um sistema de monitoramento Zabbix externo é usado para monitorar dispositivos CPE, bem como funções de rede virtual e funções de rede física. É necessário implementar um servidor Zabbix em um de seus locais ou conectar um servidor Zabbix existente e implementar servidores proxy Zabbix.

Os servidores proxy Zabbix são usados para receber resultados de monitoramento em locais individuais e enviar esses resultados de monitoramento para o servidor Zabbix. O servidor Zabbix processa os resultados de monitoramento e, em seguida, eles são exibidos na interface da Web do orquestrador.

O orquestrador usa uma API para se integrar ao servidor Zabbix. Ao registrar um dispositivo CPE ou implementar uma função de rede virtual ou uma função de rede física em um serviço de rede, um host correspondente é criado automaticamente no servidor Zabbix. É possível especificar os grupos no servidor Zabbix nos quais os hosts devem ser colocados. O host no servidor Zabbix é automaticamente excluído ao excluir o dispositivo CPE, a função de rede virtual ou a função de rede física correspondente.

Há suporte para dois métodos de monitoramento:

- O monitoramento usando agentes Zabbix envolve um componente que envia automaticamente dados de monitoramento para um servidor proxy Zabbix.
- O monitoramento via SNMP consiste no servidor proxy Zabbix estabelecendo automaticamente uma conexão com um componente via SNMP e recebendo dados de monitoramento.

Para detalhes sobre como configurar o sistema de monitoramento, consulte a documentação oficial da solução Zabbix.

Especificar o servidor Zabbix

Para especificar o servidor Zabbix:

1. No menu, acesse a seção **Sistema**.

   Por padrão, é selecionada a guia **Monitoramento**, que exibe as configurações de conexão do servidor Zabbix.

2. Selecione a guia **Monitoramento**.

   As configurações para estabelecer a conexão com o servidor Zabbix são exibidas.

3. No campo **URL**, insira a URL da API do Zabbix. O orquestrador envia solicitações HTTP para a URL especificada para receber os resultados de monitoramento e exibi-los como gráficos.

   A URL consiste no endereço da interface da Web do Zabbix e no nome do arquivo api_jsonrpc.php, usado para chamadas de API. Por exemplo, se a interface da Web do Zabbix estiver localizada em http://192.168.2.1, insira `http://192.168.2.1/api_jsonrpc.php`.

4. No campo **Nome de usuário**, insira o nome de usuário para a conexão do orquestrador à API do Zabbix. É necessário inserir o nome de usuário de uma conta que tenha permissões de leitura e gravação para grupos no servidor Zabbix, bem como permissão para criar grupos.

5. No campo **Senha**, insira a senha para estabelecer a conexão com a API do Zabbix.

6. Na lista suspensa **Agrupamento por Zabbix**, selecione um método para agrupar hosts de dispositivos CPE, assim como funções de rede virtual e funções de rede física no servidor Zabbix:

   - **Por grupos especificados** para colocar hosts de dispositivos CPE, funções de rede virtual e funções de rede física nos grupos especificados. Ao selecionar essa opção, faça o seguinte:

     a. No campo **Grupo VNF/PNF**, insira um nome de grupo para os hosts de funções de rede virtual e funções de rede física.

     b. No campo**Grupo CPE**, insira um nome de grupo para hosts de dispositivos CPE.

   - **Por locatário** para colocar hosts de dispositivos CPE, funções de rede virtual e funções de rede física em grupos criados automaticamente. Os grupos correspondem aos locatários aos quais os dispositivos CPE são adicionados e as funções de rede virtual e de rede física são atribuídas.

7. No campo **Disparar sincronização (s)**, insira o intervalo em segundos para receber notificações sobre problemas do servidor Zabbix no orquestrador. Intervalo de valores: 5 a 600. O valor padrão é `600`.

8. Abaixo do campo **Token**, clique em **Gerar** para gerar um token que as solicitações de API do servidor Zabbix para o orquestrador devem conter. Se uma solicitação de API não contiver o token, o orquestrador não aceitará tal solicitação. A segurança também é protegida por certificados TLS.

   É possível inserir o token manualmente ou visualizá-lo clicando no ícone de visualização .

9. Para verificar a disponibilidade do servidor Zabbix, clique em **Testar conexão**.

10. Clique em **Aplicar**.

O servidor Zabbix é especificado.

Especificar o servidor proxy Zabbix

Para especificar um servidor proxy Zabbix:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. No painel **Recursos**, selecione o domínio criado e, em seguida, o data center adicionado para o qual deseja especificar um servidor proxy Zabbix.

3. Selecione a guia **Recursos do sistema**.

   As configurações para estabelecer a conexão com o servidor proxy Zabbix e VNFM são exibidas.

4. Em **Proxy Zabbix**, no campo**Nome**, insira o nome do servidor proxy Zabbix. O nome deve corresponder ao nome especificado nas configurações do servidor Zabbix.

5. No campo **Endereço IP**, insira o endereço IP do servidor proxy Zabbix. O endereço IP inserido deve estar acessível para os dispositivos CPE, funções de rede virtual e funções de rede física que você deseja monitorar.

6. Clique em **Aplicar**.

O servidor proxy Zabbix é especificado.

Para excluir as configurações de conexão do servidor proxy Zabbix, clique em **Excluir**.

Configurar o monitoramento do dispositivo CPE

É possível configurar o monitoramento em um modelo de CPE. As configurações de monitoramento especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para configurar o monitoramento do dispositivo CPE:

1. No menu, acesse a seção **SD-WAN→ Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE no qual deseja configurar o monitoramento.

   A área de configurações é exibida na parte inferior da página. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Selecione a guia **Monitoramento**.

   As configurações de monitoramento do dispositivo CPE são exibidas.

4. Na lista suspensa **Tipo de monitoramento**, selecione um método de monitoramento para o dispositivo CPE:

   - **SNMP** significa monitorar usando o protocolo SNMP.
   - **Agente** significa monitoramento usando agentes Zabbix.

5. No campo **Modelo Zabbix**, insira o nome do modelo Zabbix.

6. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE.

Visualizar os resultados de monitoramento

É possível visualizar os resultados de monitoramento para uma instância SD-WAN, um dispositivo CPE, uma função de rede virtual ou uma função de rede física:

- Para visualizar os resultados de monitoramento de uma instância SD-WAN, vá para a seção **SD-WAN→Instâncias SD-WAN**, acesse a instância SD-WAN e selecione a guia **Monitoramento**.
- Para visualizar os resultados de monitoramento de um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Monitoramento**.
- Para visualizar os resultados de monitoramento de uma função de rede virtual ou física, faça login no portal de autoatendimento, vá para a seção **Catálogo** do menu e, no painel **Serviços de rede**, clique no serviço de rede implementado, clique na função de rede virtual ou física e selecione a guia **Monitoramento**.

Na lista suspensa na parte superior da área de configurações, é possível selecionar o parâmetro para o qual os resultados de monitoramento são exibidos. Para visualizar os resultados de monitoramento de um período selecionado, use os seguintes filtros de tempo:

- **Tempo real**
- **Dia**
- **Semana**
- **Mês**

Também é possível especificar o período manualmente.

Problemas de visualização

As configurações de monitoramento no servidor Zabbix determinam que problemas merecem notificações e como os problemas são classificados de acordo com o nível de gravidade. É possível visualizar a tabela de problemas no dispositivo CPE e nas configurações da função de rede virtual ou física:

- Para visualizar a tabela de problemas de um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Problemas**.
- Para visualizar a tabela de problemas de uma função de rede virtual ou física, faça login no portal de autoatendimento, vá para a seção **Catálogo** do menu e, no painel **Serviços de rede**, clique no serviço de rede implementado, clique na função de rede virtual ou física e selecione a guia **Problemas**.

As informações sobre problemas são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do problema.
- **Nível** é o nível de gravidade do problema:
  - **Média**
  - **Desastre**
  - **Alto**
  - **Informações**
  - **Não classificado**
- **Hora** é a hora em que o problema ocorreu.
- **Duração** é a duração do problema em segundos.

Visualizar o status da solução e de seus componentes

Para visualizar o status dos componentes da solução:

1. No menu, vá para a seção **Painel**.

   Os seguintes blocos de informações são exibidos:

   - **Erros em eventos** contém erros que ocorreram durante os eventos.
   - **Erros em tarefas** contém erros que ocorreram ao executar tarefas personalizadas.
   - **Sessões ativas** contém as sessões de usuário ativas.
   - **Recursos** contém informações sobre o uso de recursos de computação por componentes da solução.
   - **Solicitações de serviço** contém solicitações de serviço.
   - **CPE desconectado** contém dispositivos CPE aos quais o acesso foi perdido.
   - **Erros no CPE** contém erros encontrados por dispositivos CPE.
   - **Problemas no CPE** contém problemas encontrados por dispositivos CPE.
   - **Problemas na VNF/PNF** contém problemas encontrados por funções de rede virtual e funções de rede física.

   Se um componente da solução estiver funcionando corretamente, o widget correspondente exibirá a mensagem *Tudo está correndo bem*. Um ícone de atualização é exibido na parte superior de um bloco; quando esse ícone é clicado, as informações exibidas são atualizadas. É possível arrastar blocos com o mouse para alterar o layout.

2. Para configurar os blocos exibidos por padrão, na parte superior da página, clique no ícone de configurações → **Redefinir para o layout padrão**.

3. Para definir um intervalo de tempo diferente para a atualização das informações nos blocos:

   a. Na parte superior da página, clique no ícone de configurações → **Definir intervalo de atualização**.

   b. Na janela aberta, no campo **Atualizar o painel a cada (s)**, insira o intervalo em segundos para a atualização das informações nos blocos. Intervalo de valores: 5 a 86.400. A configuração padrão é `60`.

   c. Clique em **OK**.

   O intervalo para atualização das informações nos blocos é modificado.

Visualizar logs

É possível visualizar os logs dos componentes da solução para fins de suporte técnico. O Kaspersky SD-WAN não envia logs fora do perímetro da infraestrutura de informações de sua organização.

Para visualizar os logs:

1. No menu, acesse a seção **Logs**.

   A página de gerenciamento de logs é exibida.

2. No painel **Data centers**, selecione o data center criado ao qual os componentes da solução pertencem.

3. No painel **Recursos**, selecione o componente da solução cujo log deseja visualizar.

   O log é exibido. Por padrão, é selecionada a guia **Tarefas**, que exibe a tabela de tarefas personalizadas. As informações sobre as tarefas personalizadas são exibidas nas seguintes colunas da tabela:

   - **Ação de tarefa** é a ação da tarefa personalizada.
   - **Objeto** é o componente da solução associado à tarefa personalizada.
   - **SR** é um link para a solicitação de serviço associada à tarefa personalizada.
   - **ID do objeto** é o ID do componente da solução associado à tarefa personalizada.
   - **Nome do objeto** é o nome do componente da solução associado à tarefa personalizada.
   - **Iniciador** é o nome do usuário que executou a tarefa personalizada.
   - **IP do iniciador** é o endereço IP do usuário que executou a tarefa personalizada.
   - **Hora de início** é a data e hora em que a tarefa personalizada começou a ser executada.
   - **Término** é a data e hora em que a tarefa personalizada terminou de ser executada.

4. Para visualizar informações sobre eventos que ocorreram durante a operação de um componente da solução, selecione a guia **Eventos**.

   Uma tabela de eventos é exibida. As informações sobre eventos são exibidas nas seguintes colunas da tabela:

   - **Ação de evento** é a ação do evento.
   - **Objeto** é o componente da solução associado ao evento.
   - **SR** é um link para a solicitação de serviço associada ao evento.
   - **Nome do objeto** é o nome do componente da solução associado ao evento.
   - **ID do objeto** é o ID do componente da solução associado ao evento.
   - **Iniciador** é o nome do usuário cuja ação causou o evento.
   - **Hora** é a data e a hora em que o evento foi criado.

5. Para visualizar as solicitações de serviço de um componente da solução, selecione a guia **Solicitações de serviço**.

É exibida uma tabela de solicitações de serviço. As informações sobre solicitações de serviço são exibidas nas seguintes colunas da tabela:

- **Solicitação de serviço** é o nome da solicitação de serviço.
- **Status** é o status da solicitação de serviço.
- **Iniciador** é o nome do usuário cuja ação causou a solicitação de serviço.
- **Hora** é a data e hora em que a solicitação de serviço foi criada.

As ações que podem ser executadas com as tabelas são descritas nas instruções Gerenciar tabelas de componentes da solução.

Visualizar e excluir solicitações de serviço

As *solicitações de serviço* são tarefas executadas enquanto os componentes da solução estão funcionando e são criadas automaticamente como resultado das ações do usuário. Por exemplo, quando um usuário aplica um modelo de CPE a um dispositivo CPE, uma solicitação de serviço correspondente é criada. Cada solicitação de serviço consiste em várias etapas que são executadas em sequência.

Visualizar solicitações de serviço

É possível visualizar as solicitações de serviço de um locatário, um dispositivo CPE e uma instância SD-WAN:

- Para visualizar as solicitações de serviço de um locatário, vá para a seção **Locatários** e, em **Locatários**, selecione um locatário.

  A lista de solicitações de serviço é exibida em **Solicitações de serviço**.

- Para visualizar as solicitações de serviço de uma instância SD-WAN, vá para a seção **SD-WAN→Instâncias SD-WAN**, acesse a instância SD-WAN e selecione a guia **Solicitações de serviço**.

  É exibida uma tabela de solicitações de serviço.

- Para visualizar as solicitações de serviço de um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE e selecione a guia **Solicitações de serviço**.

  É exibida uma tabela de solicitações de serviço.

A lista de solicitações de serviço de um locatário exibe o nome e a ID da solicitação de serviço, bem como a data e hora de criação. As informações sobre solicitações de serviço de uma instância SD-WAN e um dispositivo CPE são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da solicitação de serviço.
- **Criado** é a data e hora em que a solicitação de serviço foi criada.
- **ID da tarefa** é o ID da solicitação de serviço.
- **Hora** é a duração da solicitação de serviço em segundos.
- **Status** é o status da solicitação de serviço:

- **Executando** significa que a solicitação de serviço está sendo executada.
- **Não executado** significa que ocorreu um erro ao executar a solicitação de serviço.
- **Executado** significa que a solicitação de serviço foi executada com êxito.
- **Revertendo** significa que ocorreu um erro ao executar uma das etapas da solicitação de serviço, portanto, as etapas já executadas estão sendo revertidas.
- **Não revertido** significa que ocorreu um erro ao reverter uma das etapas da solicitação de serviço executadas anteriormente.
- **Revertido** significa que as etapas da solicitação de serviço executadas anteriormente foram revertidas com êxito.
- **Suspensa** significa que ocorreu um erro ao executar a solicitação de serviço para registrar o dispositivo CPE e o registro do dispositivo CPE não foi concluído. É possível retomar o registro do dispositivo CPE.

- **Ações** contém as ações que podem ser executadas com as solicitações de serviço.

É possível abrir o log da solicitação de serviço:

- Para abrir o log de uma solicitação de serviço de locatário, clique no nome da solicitação de serviço.
- Para abrir o log de uma solicitação de serviço para uma instância SD-WAN ou um dispositivo CPE, clique no ID da solicitação de serviço.

Um log da solicitação de serviço é exibido.

O log contém informações sobre as etapas em que ocorreram erros. Clique na etapa em que o erro ocorreu para visualizar uma descrição detalhada dele.

Excluir solicitações de serviço

É possível excluir solicitações de serviço de uma instância SD-WAN ou um dispositivo CPE. Apenas solicitações de serviço com status diferente de **Suspensa** são excluídos. A exclusão de uma solicitação de serviço interrompe a operação associada.

As solicitações de serviço excluídas não podem ser restauradas.

Para excluir uma solicitação de serviço, execute uma das seguintes ações:

- Para excluir uma única solicitação de serviço, clique em **Excluir** ao lado dela.
- Para excluir todas as solicitações de serviço, na parte superior da área de configurações, em **Ações**, clique em **Excluir tudo**.

Confirme a exclusão clicando no botão **Excluir** na janela exibida.

As solicitações de serviço são excluídas e não são mais exibidas na tabela.

Enviar notificações de dispositivos CPE aos usuários

O Kaspersky SD-WAN pode enviar notificações aos endereços de e-mail dos usuários com as seguintes informações sobre os dispositivos CPE:

- Eventos do log:
  - Ativar e desativar um dispositivo CPE
  - Conectar ou desconectar uma porta
  - Conectar ou desconectar um link
- Problemas:
  - Problemas encontrados
  - Problemas resolvidos

As informações são acumuladas por cinco segundos antes que a notificação seja enviada. Por exemplo, se a desconexão de uma porta fizer com que cinco links sejam desconectados, essas informações devem ser acumuladas e enviadas ao usuário na mesma notificação.

Especifique o servidor SMTP a ser usado por todos os usuários para o envio de notificações. No portal do administrador, é possível configurar notificações sobre eventos e problemas para todos os locatários. No portal de autoatendimento, é possível configurar notificações sobre eventos e problemas para um único locatário.

Especificar o servidor SMTP

Para especificar um servidor SMTP:

1. No menu, acesse a seção **Sistema**.

   Por padrão, é selecionada a guia **Monitoramento**, que exibe as configurações de conexão do servidor Zabbix.

2. Selecione a guia **Notificação** → **SMTP**.

   As configurações de conexão do servidor SMTP são exibidas.

3. Marque a caixa de seleção **Ativar** para usar o servidor SMTP. Esta caixa de seleção está desmarcada por padrão.

4. No campo **Servidor SMTP**, insira o endereço IP ou o nome de domínio do servidor SMTP.

5. No campo **Porta do servidor SMTP**, insira o número da porta do servidor SMTP. Intervalo de valores: 0 a 65.535. O valor padrão é `25`.

6. No campo **E-mail do remetente**, insira o endereço de e-mail a partir do qual o servidor SMTP envia notificações aos usuários.

7. Para configurar a criptografia da conexão entre o Kaspersky SD-WAN e o servidor SMTP, na lista suspensa **SSL/TLS**, selecione um dos seguintes valores:

   - **Nenhum** para deixar a conexão sem criptografia. Essa é a configuração padrão.
   - **STARTTLS** para determinar o método de criptografia e, em seguida, estabelecer uma conexão criptografada.
   - **SMTPS** para estabelecer uma conexão criptografada imediatamente.

8. Para ativar a autenticação do Kaspersky SD-WAN no servidor SMTP:

   a. Marque a caixa de seleção **Autenticação**. Esta caixa de seleção está desmarcada por padrão.

   b. No campo **Nome de usuário**, insira o nome de usuário que o Kaspersky SD-WAN usa para fazer a autenticação no servidor SMTP. O comprimento máximo do nome é de 64 caracteres.

   c. No campo **Senha**, insira a senha que o Kaspersky SD-WAN usa para fazer a autenticação no servidor SMTP. O comprimento máximo da senha é de 64 caracteres. Para ver a senha inserida, clique no ícone de exibição .

9. Para enviar uma mensagem de teste usando o servidor SMTP:

   a. Clique em **Teste**.

   b. Na janela aberta, insira o endereço de e-mail para o qual deseja que o servidor SMTP envie uma mensagem de teste.

   c. Clique em **Enviar**.

   Uma mensagem de teste é enviada para o endereço de e-mail especificado com *Teste de notificação* no assunto e no corpo.

10. Clique em **Aplicar**.

    O servidor SMTP é especificado.

Configurar notificações

O administrador da plataforma deve especificar o servidor SMTP para ativar o envio de notificações ao usuário.

Para configurar notificações:

1. No menu, acesse a seção **Sistema**.

   Por padrão, é selecionada a guia **Monitoramento**, que exibe as configurações de conexão do servidor Zabbix.

2. Selecione a guia **Notificação** → **Alerta**.

   As configurações de notificação são exibidas.

3. Marque a caixa de seleção **Ativar** para enviar notificações ao usuário. Esta caixa de seleção está desmarcada por padrão.

4. No campo **Endereço de e-mail do receptor**, insira o endereço de e-mail para o qual deseja enviar notificações.

5. No campo **Assunto**, insira o texto do assunto dos e-mails de notificação. O comprimento máximo do tópico é de 64 caracteres.

6. Clique em **Aplicar**.

As notificações serão enviadas para o endereço de e-mail especificado.

Selecionar o detalhamento do log do contêiner Docker

O Kaspersky SD-WAN mantém automaticamente os logs dos contêineres Docker do controlador e do orquestrador. É possível selecionar o detalhamento do log de contêiner Docker.

Para selecionar o detalhamento do log do contêiner Docker:

1. Selecione o nível de detalhamento do log do contêiner Docker de uma das seguintes formas:

   - Para selecionar o detalhamento do log do contêiner Docker para o controlador: no menu, acesse a seção **Infraestrutura**, clique em **Gerenciamento**→ **Configurações de implementação** ao lado do controlador e vá para a seção **Logs**.

   - Para selecionar o detalhamento do log do contêiner Docker para o orquestrador: no menu, vá para seção **Sistema** e selecione a guia **Log do orquestrador**.

   Isso abre uma página com uma tabela de contêineres Docker. As informações sobre os contêineres Docker são exibidas nas seguintes colunas da tabela:

   - **Nome do módulo** é o nome do contêiner Docker.

   - **Nível do registro** é o detalhamento do log do contêiner Docker:

   Para encontrar o contêiner Docker, insira o nome dele no campo **Filtrar**.

2. Selecione o nível de detalhamento do contêiner Docker de uma das seguintes formas:

   - Para selecionar o nível de detalhamento de todos os contêineres Docker, clique no botão correspondente na seção **Nível geral do registro**.

   - Para selecionar o nível de detalhamento de um único contêiner Docker, clique no botão correspondente ao lado dele.

   É possível selecionar os seguintes níveis de detalhamento para contêineres Docker:

   - **RASTREIO** para que o log inclua as informações mais completas sobre a operação e a condição do módulo e suas variáveis. Use esse nível de detalhe para observar a execução do código, bem como para diagnóstico e análise detalhada de erros que ocorrem durante o desenvolvimento.

   - **DEPURAÇÃO** para que o log inclua as informações necessárias para depurar o módulo, como o status das operações e os valores das variáveis. Use esse nível de detalhe para diagnosticar erros e analisar o comportamento do módulo.

   - **INFO** para que o log inclua informações gerais necessárias para entender o funcionamento do módulo, por exemplo, confirmações de operações. Use esse nível de detalhe para rastrear o andamento da execução do módulo. Esse nível de detalhe é selecionado por padrão para todos os contêineres.

- **AVISO** para que o log inclua informações sobre incidentes que não são erros, mas que podem comprometer a operação do contêiner e exigir uma intervenção de sua parte, como problemas com configurações e funções obsoletas. Use esse nível de detalhe para evitar possíveis erros.

- **ERRO** para que o log inclua informações sobre erros que ocorrem durante a execução do código e exigem uma intervenção de sua parte. Uma mensagem de erro pode conter informações sobre a parte do contêiner em que o erro ocorreu, bem como informações detalhadas sobre o erro. Use esse nível de detalhe para resolver erros que ocorram.

O nível de detalhamento do log do contêiner Docker é modificado.

Monitorar dispositivos CPE, VNF e PNF usando o SNMP

É possível usar o SNMP para monitorar dispositivos CPE, bem como funções de rede virtual e funções de rede física. É necessário instalar um agente SNMP no componente que deseja monitorar. O agente SNMP reúne dados de monitoramento e os envia ao gerenciador de SNMP para processamento. No Kaspersky SD-WAN, o servidor proxy Zabbix atua como gerenciador de SNMP.

O gerenciador de SNMP e os agentes SNMP trocam solicitações e notificações. Por padrão, os agentes SNMP recebem solicitações do gerenciador de SNMP na porta 161. No entanto, o gerenciador de SNMP pode enviar solicitações por meio de qualquer porta disponível. A resposta chega na mesma porta de onde a solicitação foi enviada.

Por padrão, o gerenciador de SNMP recebe notificações de agentes SNMP na porta 162. No entanto, os agentes SNMP podem enviar notificações por meio de qualquer porta disponível. Existem dois tipos de notificações:

- *Interceptações* são notificações sobre eventos que o agente SNMP envia sem uma solicitação prévia do gerenciador de SNMP. Quando ocorre um evento especificado, como o desligamento de um dispositivo CPE ou de uma de suas interfaces de rede, o agente SNMP gera uma interceptação e a envia ao gerenciador de SNMP como uma mensagem UPD. As interceptações permitem informar automaticamente o gerenciador de SNMP sobre eventos, sem esperar por uma solicitação.

- *Solicitações de informação* são notificações semelhantes a interceptações, mas que diferem porque exigem uma confirmação adicional do gerenciador de SNMP. Quando o agente SNMP envia uma solicitação de informação ao gerenciador de SNMP, ele aguarda o recebimento de uma confirmação. Se o gerenciador de SNMP receber e processar com êxito a solicitação de informação, ele envia uma mensagem de confirmação ao agente SNMP. O mecanismo de confirmação permite garantir a confiabilidade na entrega de notificações.

Ao usar o protocolo TLS ou DTLS, as interceptações chegam na porta 10162 do gerenciador de SNMP e as solicitações de informação chegam na porta 10161.

Todas as unidades de dados de protocolo (PDUs) básicas têm a mesma estrutura (veja a figura abaixo). O cabeçalho IP e o cabeçalho UDP são usados para encapsulamento e não fazem, de fato, parte da unidade de dados do protocolo.

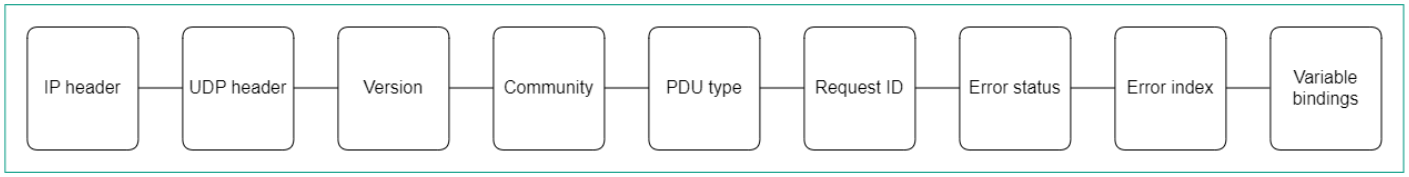


Diagrama de unidade de dados do protocolo SNMP

Para visualizar a tabela de interceptações, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador ao qual os componentes que você deseja monitorar estão conectados e vá para a seção **SNMP**. As informações sobre interceptações são exibidas nas seguintes colunas da tabela:

- **#** é o número de série da interceptação.
- **IP do gerenciador** é o endereço IP ou o nome do host do gerenciador de SNMP.
- **Porta do gerenciador** é o número da porta do gerenciador de SNMP.
- **Comunidade** é a string da comunidade SNMP.
- **Interceptações permitidas** são interceptações que os agentes SNMP devem enviar ao gerenciador de SNMP.
- **Descrição** é uma breve descrição da interceptação.

Configurar a conexão entre o gerenciador de SNMP e os agentes SNMP

É necessário especificar as configurações para conectar o gerenciador de SNMP aos agentes SNMP instalados em dispositivos CPE, bem como nas funções de rede virtual e física. As configurações especificadas são usadas por todos os agentes SNMP.

Para configurar a conexão entre o gerenciador de SNMP e os agentes SNMP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador ao qual os componentes que deseja monitorar estão conectados.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **SNMP**.

   Uma tabela de interceptações é exibida.

4. Na parte superior da página, em **Parâmetros do gerenciador**, clique em **Editar**.

5. Na janela aberta, no campo **Endereço**, insira o endereço IP ou o nome do host do equipamento em que o agente SNMP está instalado, no formato `<protocolo de transporte>:<endereço IP ou nome do host>/<número da porta>`. Por exemplo, `udp:192.168.2.0/24`.

6. No campo **Comunidade**, insira a string da comunidade SNMP. A string de comunidade SNMP é usada como senha que o gerenciador de SNMP utiliza para se conectar aos agentes SNMP. Valor padrão: `público` significa que é concedido acesso somente leitura. Recomendamos alterar o padrão para uma string de comunidade exclusiva de forma a garantir a segurança da comunicação entre o gerenciador de SNMP e os agentes SNMP.

   Especifique a mesma string de comunidade ao configurar a conexão do gerenciador de SNMP aos agentes SNMP e ao criar ou editar interceptações.

7. Clique em **Salvar**.

A conexão do gerenciador de SNMP aos agentes é configurada.

Criar uma interceptação

É possível criar uma interceptação que os agentes SNMP devem enviar ao gerenciador de SNMP.

Para criar uma interceptação:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. Clique em **Gerenciamento → Configurações de implementação** ao lado do controlador ao qual os componentes que deseja monitorar estão conectados.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **SNMP**.

   Uma tabela de interceptações é exibida.

4. Em **Parâmetros de interceptação**, clique em **Editar**.

5. Na janela aberta, clique em **+ Adicionar** para criar uma interceptação.

6. No campo **IP do gerenciador**, insira o endereço IP ou o nome do host do gerenciador de SNMP. Intervalo de valores: 1 a 255.

7. No campo **Porta do gerenciador**, insira o número da porta do gerenciador de SNMP. Intervalo de valores: 1 a 65.534. O valor padrão é `162`.

8. No campo **Comunidade**, insira a string da comunidade SNMP. A string de comunidade SNMP é usada como senha que o gerenciador de SNMP utiliza para se conectar aos agentes SNMP. Valor padrão: `público` significa que é concedido acesso somente leitura. Recomendamos alterar o padrão para uma string de comunidade exclusiva de forma a garantir a segurança da comunicação entre o gerenciador de SNMP e os agentes SNMP.

   Especifique a mesma string de comunidade SNMP ao configurar a conexão do gerenciador de SNMP aos agentes SNMP e ao criar ou editar interceptações.

9. No campo **Interceptações permitidas**, clique em **Editar** e desmarque as seguintes caixas de seleção para especificar quais interceptações os agentes SNMP não enviam ao gerenciador de SNMP:

   - Desmarque a caixa de seleção **Interceptar quando uma interface estiver ativa** para impedir que o agente SNMP envie uma interceptação ao gerenciador SNMP quando uma das portas do componente no qual o agente SNMP está instalado se tornar ativa.
   - Desmarque a caixa de seleção **Interceptar quando uma interface estiver inativa** para impedir que o agente SNMP envie uma interceptação ao gerenciador SNMP quando uma das portas do componente no qual o agente SNMP está instalado se tornar inativa.
   - Desmarque a caixa de seleção **Interceptar quando equipamentos estiverem ativos** para impedir que o agente SNMP envie uma interceptação ao gerenciador SNMP quando o componente no qual o agente SNMP está instalado se tornar ativo.
   - Desmarque a caixa de seleção **Interceptar quando equipamentos estiverem inativos** para impedir que o agente SNMP envie uma interceptação ao gerenciador SNMP quando o componente no qual o agente SNMP está instalado se tornar inativo.

   Por padrão, as caixas de seleção são marcadas.

10. Clique em **Voltar** para continuar especificando as configurações de interceptação.
11. No campo **Descrição**, insira uma breve descrição da interceptação.
12. Clique em **Salvar**.

A interceptação é criada e exibida na tabela.

Editar uma interceptação

Para editar uma interceptação:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. Clique em **Gerenciamento → Configurações de implementação** ao lado do controlador ao qual os componentes que deseja monitorar estão conectados.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **SNMP**.

   Uma tabela de interceptações é exibida.

4. Em **Parâmetros de interceptação**, clique em **Editar**.
5. Na janela aberta, se necessário, edite as configurações da interceptação. Para obter uma descrição das configurações, consulte as instruções para criar uma interceptação.
6. Clique em **Salvar**.

A interceptação é modificada e atualizada na tabela.

Excluir uma interceptação

As interceptações excluídas não podem ser restauradas.

Para excluir uma interceptação:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores SD-WAN.

2. Clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador ao qual os componentes que deseja monitorar estão conectados.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **SNMP**.

   Uma tabela de interceptações é exibida.

4. Em **Parâmetros de interceptação**, clique em **Editar**.

5. Na janela aberta, clique em **Excluir** ao lado da interceptação que deseja excluir.

6. Clique em **Salvar**.

A interceptação é excluída e não é mais exibida na tabela.

Monitoramento de links

Para ativar o monitoramento de links:

1. Ative o monitoramento de links de uma das seguintes formas:

   - Para ativar o monitoramento de um link estabelecido a partir de um dispositivo CPE, vá para a seção **SD-WAN**→ **CPE**, clique no dispositivo CPE, selecione a guia **Links** e clique em **Gerenciamento** → **Definir limites** ao lado do link.

   - Para ativar o monitoramento de um dos links na tabela com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador, vá para a seção **Links** e clique em **Gerenciamento** → **Definir limites** ao lado do link.

   - Para ativar o monitoramento de um dos links na topologia gráfica com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador, vá para a seção **Topologia**, clique no link e, então, em **Definir limites**.

2. Marque a caixa de seleção **Ativar monitoramento de limite** para ativar o monitoramento do link. Esta caixa de seleção está desmarcada por padrão.

3. Para especificar limites de monitoramento de links:

   a. Para definir limites de monitoramento de link padrão, clique em **Definir para padrão**.

   b. Caso deseje que o controlador use o link como o último recurso ao calcular caminhos, independentemente dos limites de monitoramento, marque a caixa de seleção **Último recurso**. Esta caixa de seleção está desmarcada por padrão.

   c. No campo **Intervalo para erros de processamento e taxa de utilização (s)**, insira o intervalo de tempo em segundos para medir o número de erros no link e seu nível de utilização. Intervalo de valores: 1 a 300. O valor padrão é `60`.

   d. Para especificar um limite para o número de erros por segundo no link, marque a caixa de seleção **Ativar monitoramento de erros** e, no campo **Nível de erro crítico (erros/s)**, insira o valor-limite. Intervalo de valores: 1 a 1.000.000. Essa caixa de seleção é desmarcada por padrão e o valor no campo é `1000`.

   e. Para especificar um limite para a utilização do link na forma de uma porcentagem da taxa de bits da interface de serviço de origem, marque a caixa de seleção **Ativar monitoramento de utilização** e, no campo **Nível de utilização crítico (%)**, insira o valor-limite. Essa caixa de seleção é desmarcada por padrão e o valor no campo é `95`.

   f. No campo **Intervalo para latência de processamento, jitter e perda de pacotes (s)**, insira o intervalo de tempo em segundos para medir latência, jitter e perda de pacotes no link. Intervalo de valores: 1 a 600. O valor padrão é `30`.

   g. Para especificar um limite de latência em milissegundos para a transmissão do tráfego pelo link, marque a caixa de seleção **Ativar monitoramento de latência** e, no campo **Nível crítico de latência (ms)**, insira o valor-limite. Intervalo de valores: 5 a 1000. Essa caixa de seleção é desmarcada por padrão e o valor no campo é `100`.

   h. Para especificar um limite de tempo de jitter em milissegundos para a transmissão do tráfego pelo link, marque a caixa de seleção **Ativar monitoramento de jitter** e, no campo **Nível crítico de jitter (ms)**, insira o valor-limite. Intervalo de valores: 5 a 1000. Essa caixa de seleção é desmarcada por padrão e o valor no campo é `100`.

   i. Para especificar um limite para a porcentagem de pacotes de tráfego perdidos no link, marque a caixa de seleção **Ativar monitoramento de perda de pacotes** e, no campo **Nível crítico de perda de pacotes (%)**, insira o valor-limite. Intervalo de valores: 1 a 100. Essa caixa de seleção é desmarcada por padrão e o valor no campo é `2`.

   Os limites de monitoramento especificados são usados pelas restrições de limite.

4. Salve as configurações de monitoramento de links de uma das seguintes formas:

   - Para salvar as configurações de monitoramento de links, clique em **Salvar**.
   - Para salvar as configurações de monitoramento de links e especificar as mesmas configurações no link de direção oposta, clique em **Salvar para ambos os links**.

5. Caso tenha especificado as configurações de monitoramento de um link estabelecido a partir do dispositivo CPE, clique em **Salvar** na parte superior da área de configurações para salvar as configurações do dispositivo CPE.

Construir uma rede SD-WAN entre dispositivos CPE

Para transferir o tráfego, é necessário construir uma rede SD-WAN entre dispositivos CPE usando links estabelecidos sobre a rede underlay. Os dispositivos CPE estabelecem links a partir de todas as interfaces SD-WAN do tipo WAN disponíveis. Os links são unidirecionais. Isso significa que ao estabelecer um link do CPE 1 ao CPE 2, um link também é automaticamente estabelecido do CPE 2 ao CPE 1. Antes de construir uma rede SD-WAN, garanta a conectividade entre os dispositivos CPE.

Os links são estabelecidos com base nas funções atribuídas aos dispositivos CPE. É possível atribuir a função de Gateway SD-WAN ou a função de dispositivo CPE padrão a um dispositivo CPE. Gateways SD-WAN estabelecem links com todos os dispositivos CPE padrão e outros Gateways SD-WAN. Dispositivos CPE padrão estabelecem links somente com Gateways SD-WAN. Por padrão, todos os dispositivos CPE têm a função de dispositivo CPE padrão.

Para que um link seja estabelecido entre dois dispositivos CPE padrão, é necessário atribuir a mesma tag de topologia a eles. É possível transformar um dispositivo CPE padrão em um dispositivo de trânsito para permitir que outros dispositivos CPE estabeleçam links por meio dele.

Os links entre os dispositivos CPE formam uma topologia. As seguintes topologias são as mais usadas no Kaspersky SD-WAN:

- Em uma topologia Hub-and-Spoke, os links entre dispositivos CPE são estabelecidos por meio de gateways SD-WAN.

- Nas topologias Full-Mesh e Partial-Mesh, os links entre dispositivos CPE são estabelecidos diretamente, ou alguns links são estabelecidos diretamente, enquanto outros são estabelecidos por meio de gateways SD-WAN.

Na rede SD-WAN, o tráfego entre dispositivos CPE pode tomar vários caminhos. Os caminhos passam pelos links entre dispositivos CPE. A totalidade de todos os caminhos possíveis entre dois dispositivos CPE é chamada de *segmento*. O dispositivo CPE de origem do segmento pode distribuir o tráfego vinculado ao dispositivo CPE de destino do segmento por vários caminhos. Um segmento pode conter de 2 a 16 caminhos.

Os seguintes tipos de caminho são compatíveis:

- *Auto-SPF* (Shortest-Path Forwarding) é um caminho calculado automaticamente pelo controlador. É possível encaminhar o tráfego ao longo dos caminhos Auto-SPF de dois modos:

  - No modo *Ativo/Ativo*, vários caminhos Auto-SPF são usados simultaneamente para encaminhar o tráfego entre dispositivos CPE.

  - No modo *Ativo/Espera*, um caminho de Auto-SPF com o custo mais baixo é usado para encaminhar o tráfego entre dispositivos CPE. Se o caminho de Auto-SPF usado se tornar indisponível, o caminho de Auto-SPF com o próximo custo mais baixo será usado. O custo do caminho é calculado somando o custo de cada link percorrido pelo caminho. É possível especificar o custo do link manualmente.

  É possível configurar o modo de encaminhamento de tráfego ao longo dos caminhos Auto-SPF ao configurar os caminhos.

- *Auto-TE* (Engenharia de Tráfego) é um caminho calculado automaticamente pelo controlador, levando em consideração as restrições de limite especificadas.

- *Manual-TE* é um caminho criado manualmente. Ao criar um caminho de Manual-TE, especifique os links pelos quais o caminho passa do dispositivo CPE de origem ao dispositivo CPE de destino do segmento.

Sobre a topologia Hub-and-Spoke

Em uma topologia Hub-and-Spoke, o site hub é conectado a vários sites spoke para trocar tráfego. Essa topologia é a mais comum para o projeto da rede SD-WAN pois simplifica o gerenciamento da rede e fornece um nível mais alto de segurança ao rotear o tráfego através do site hub no qual a análise e a categorização do tráfego são executadas. A topologia Hub-and-Spoke também permite o uso mais eficiente da largura de banda ao otimizar e priorizar o tráfego no site hub.

Para criar uma topologia Hub-and-Spoke, é necessário atribuir o gateway SD-WAN e as funções CPE padrão aos dispositivos CPE. Nesse caso, os gateways SD-WAN estabelecem links com outros gateways SD-WAN e dispositivos CPE padrão, enquanto os dispositivos CPE padrão estabelecem links apenas com gateways SD-WAN.

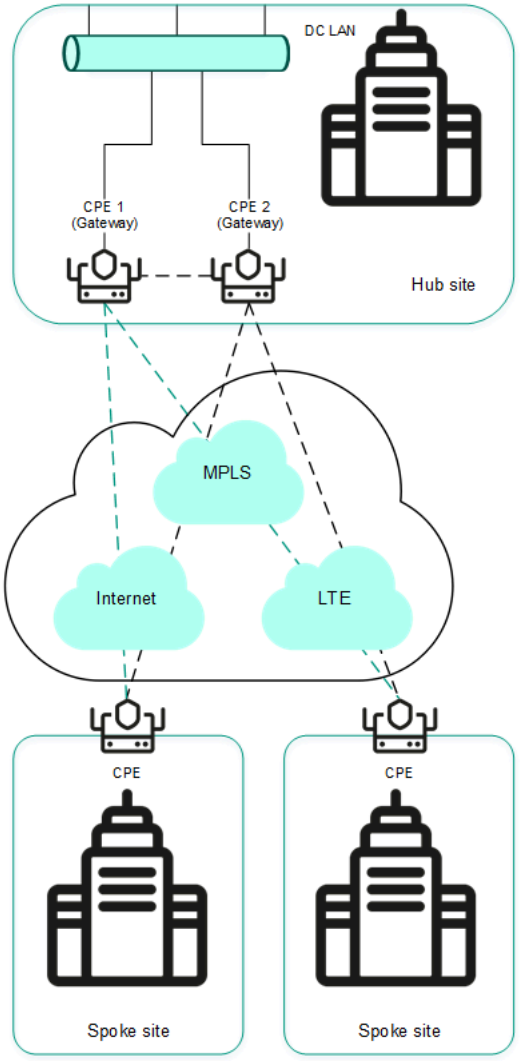
É possível usar a qualidade de serviço para limitar a largura de banda para dispositivos CPE ou classes de tráfego.

Exemplos de topologias Hub-and-Spoke:

- **Topologia Hub-and-Spoke sem conexão entre sites spoke**.

  A figura abaixo mostra uma topologia Hub-and-Spoke na qual os sites spoke se comunicam com o site hub, mas não entre si. As redes SD-WAN criadas usando essa topologia são fáceis de projetar e manter, pois todos os serviços de rede e aplicativos necessários estão localizados no mesmo data center.

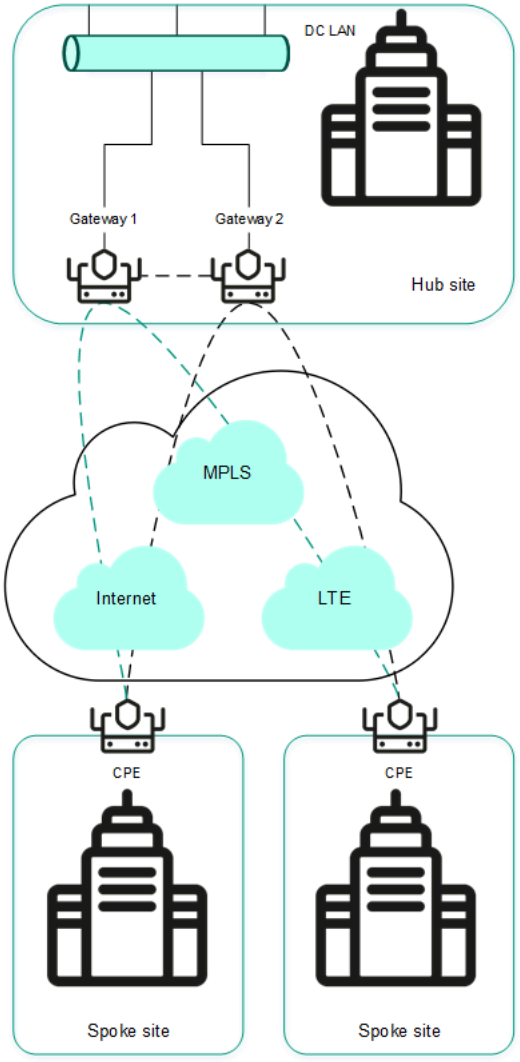
Os dispositivos CPE sendo registrados são automaticamente incluídos no serviço de transporte de gerenciamento com a função de Folha e podem estar por trás da NAT (Conversão de endereço de rede) e PAT (Conversão de endereço de porta). Nessa topologia Hub-and-Spoke, o tráfego não pode ser transmitido diretamente entre dispositivos CPE.



Topologia Hub-and-Spoke sem conexão entre sites spoke

- **Topologia Hub-and-Spoke com conexão entre sites spoke através do site hub**.

  A figura abaixo mostra uma topologia Hub-and-Spoke na qual os sites spoke podem se comunicar entre si através do site hub. Os dispositivos CPE sendo registrados são automaticamente adicionados ao serviço de transporte de gerenciamento e podem estar atrás da NAT e PAT.



Topologia Hub-and-Spoke com conexão entre sites spoke por meio do site hub

Sobre as topologias Full-Mesh e Partial-Mesh

Nas topologias Full-Mesh e Partial-Mesh, os links são estabelecidos entre dispositivos CPE padrão. O estabelecimento de links entre dispositivos CPE padrão tem as seguintes vantagens sobre uma topologia Hub-and-Spoke, na qual os dispositivos CPE padrão devem se comunicar por meio de gateways SD-WAN:

- Melhoria de aspectos de qualidade de links, como atraso, perda de pacotes e jitter.
- Maior largura de banda de links.
- Economia de recursos de hardware de gateways SD-WAN.

Para criar uma topologia Full-Mesh, é necessário atribuir a função de dispositivo CPE padrão aos dispositivos CPE e atribuir a mesma tag de topologia aos dispositivos CPE padrão. Nesse caso, os dispositivos CPE padrão com as mesmas tags de topologia estabelecem links uns com os outros.

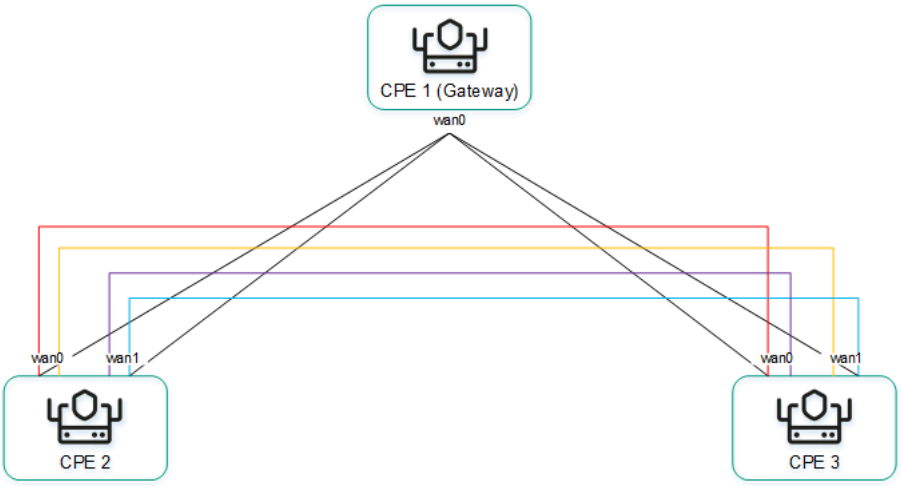
Para criar uma topologia Partial-Mesh, é necessário atribuir o gateway SD-WAN e as funções de dispositivo CPE padrão aos dispositivos CPE e atribuir a mesma tag de topologia aos dispositivos CPE padrão. Nesse caso, os gateways SD-WAN estabelecem links com outros gateways SD-WAN e com dispositivos CPE padrão, enquanto os dispositivos CPE padrão estabelecem links com gateways SD-WAN e entre si, desde que a mesma tag de topologia seja atribuída aos dispositivos CPE padrão. Caso deseje dividir os dispositivos CPE padrão em grupos, é necessário atribuir uma tag de topologia exclusiva a todos os dispositivos CPE padrão em cada grupo, além de atribuir uma tag de topologia a ser compartilhada por pelo menos um dispositivo CPE padrão em cada grupo.

É possível usar a qualidade de serviço para limitar a largura de banda para dispositivos CPE ou classes de tráfego.

Exemplos de topologia Full-Mesh e Partial-Mesh:

- **Topologia Full-Mesh**.

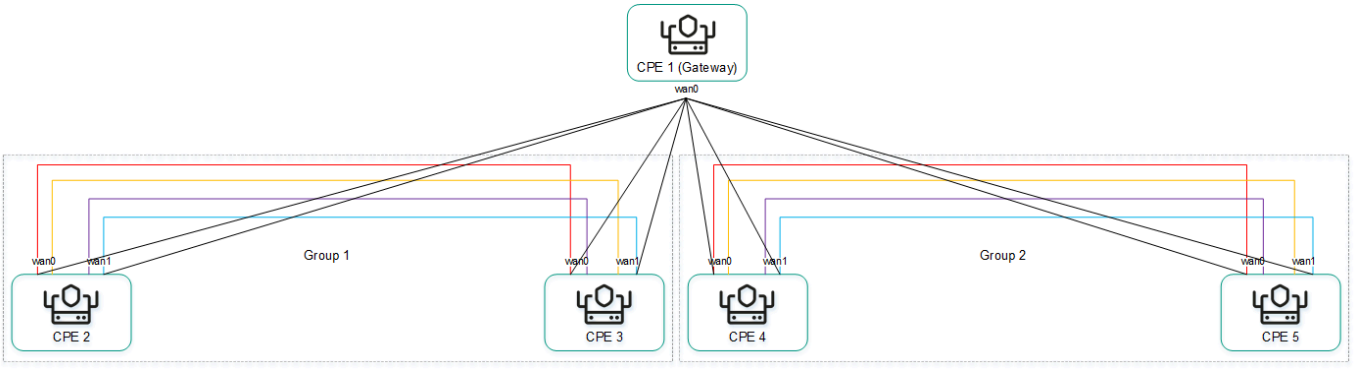
  A figura abaixo mostra uma topologia Full-Mesh na qual todos os dispositivos CPE estabelecem links entre si. O tráfego entre os dispositivos CPE 2 e CPE 3 é encaminhado diretamente. Com muitos dispositivos CPE e links, essa topologia pode ser extremamente desgastante para os recursos do controlador.



Topologia Full-Mesh

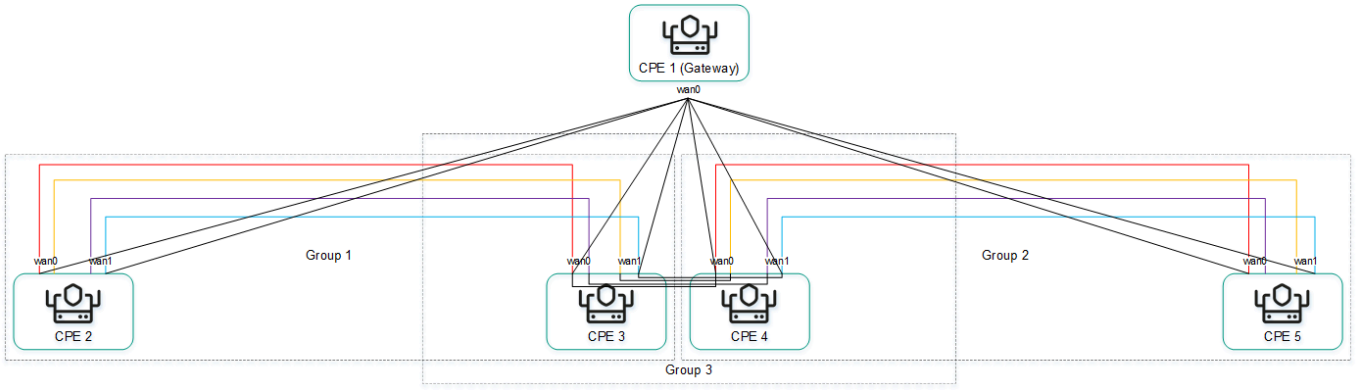
- **Topologia Partial-Mesh**.

  A figura abaixo mostra uma topologia Partial-Mesh. Essa topologia é usada quando links diretos entre alguns dispositivos CPE podem não ser desejáveis, por motivos administrativos, ou impossíveis, por motivos técnicos. Nessa topologia, é possível agrupar dispositivos CPE de forma que os dispositivos no mesmo grupo se comuniquem diretamente entre si e com dispositivos CPE de outros grupos por meio de um dispositivo CPE de trânsito.



Topologia Partial-Mesh

Um dispositivo CPE pode fazer parte de vários grupos ao mesmo tempo, conforme mostrado na figura abaixo.

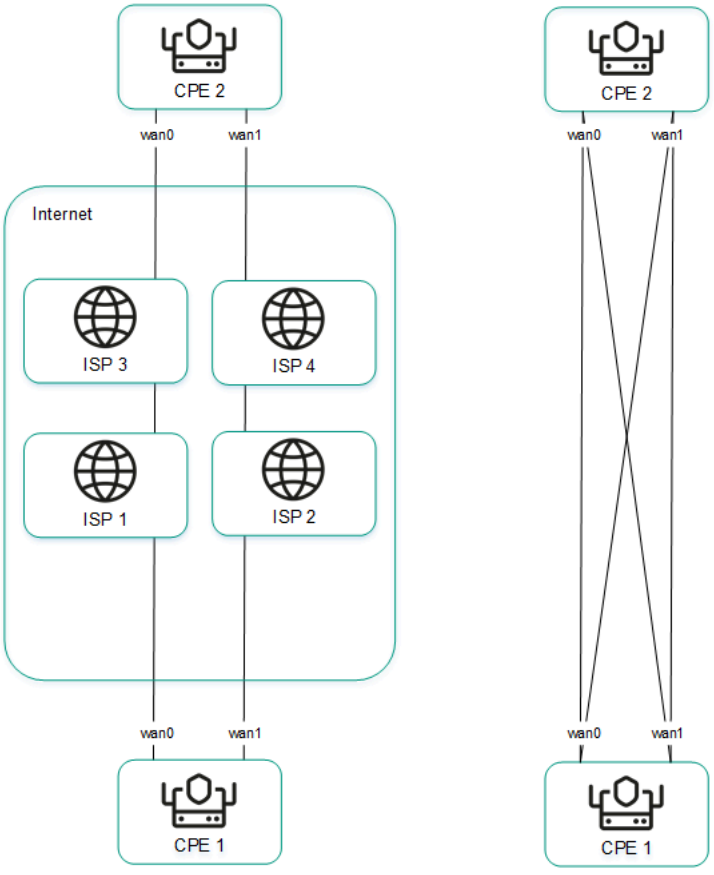


Topologia Partial-Mesh, dispositivos CPE em grupos diversos

Ao criar links diretos entre dispositivos CPE, dependendo do tipo de conexão dos dispositivos CPE por meio de links físicos, as seguintes variantes de conectividade overlay são possíveis:

- **Todos os links físicos têm conectividade IP direta entre si**.

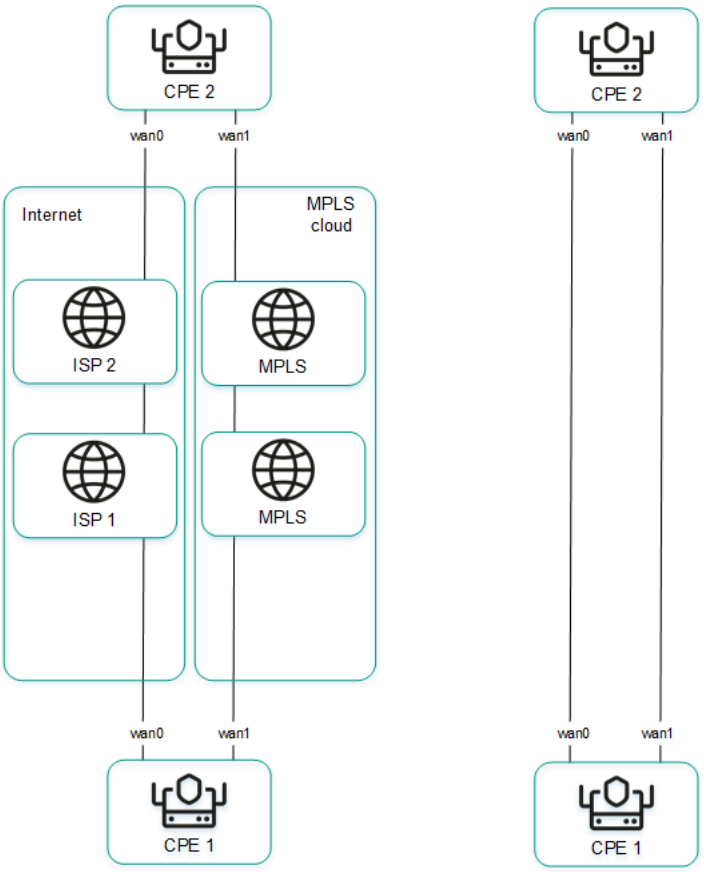
  Graças à conectividade na Internet, os dispositivos CPE podem estabelecer o número máximo de links entre si (veja a figura abaixo).



Conexão física completa entre dispositivos CPE

- **Os links físicos têm conectividade IP parcial entre si**.

  Na figura abaixo, a nuvem da Internet e a nuvem MPLS não estão conectadas entre si, portanto, os links só podem ser estabelecidos por meio de interfaces SD-WAN do tipo WAN que pertencem à mesma nuvem. Os links CPE1:WAN0 → CPE2:WAN1 e CPE1:WAN1 → CPE2:WAN0 não podem ser estabelecidos.



Outros cenários de conectividade de rede overlay também são possíveis se a conexão IP entre interfaces SD-WAN do tipo WAN de dispositivos CPE dentro da mesma nuvem não for possível por outros motivos, por exemplo, ao usar uma topologia MPLS sem suporte à comunicação direta entre dispositivos CPE, ou devido à presença de NAT/PAT ou ACL na Internet.

Atribuir uma função a um dispositivo CPE

É possível atribuir uma função a um modelo de CPE ou a um dispositivo CPE. Uma função atribuída a um modelo de CPE é automaticamente atribuída a todos os dispositivos CPE que usam o modelo.

Para atribuir uma função a um dispositivo CPE:

1. Atribua uma função a um dispositivo CPE de uma das seguintes formas:

   - Para atribuir uma função a um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Topologia**.

   - Para atribuir uma função a um dispositivo CPE, execute uma das seguintes ações:

     - No menu, acesse a seção **SD-WAN → CPE**, clique no dispositivo CPE, selecione a guia **Topologia** e marque a caixa de seleção **Substituir**.

     - No menu, acesse a seção **Infraestrutura**, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador, vá para a seção **Tags de topologia** e, na lista suspensa **Switch**, selecione o dispositivo CPE.

2. Na lista suspensa **Função**, selecione a função do dispositivo CPE:

   - **CPE** para um dispositivo CPE padrão. Essa é a configuração padrão.
   - **Gateway** para um gateway SD-WAN. Não é possível atribuir tags de topologia a gateways SD-WAN.

3. Salve a função do dispositivo CPE de uma das seguintes formas:

   - Caso tenha atribuído uma função a um modelo de CPE ou a um dispositivo CPE na seção **SD-WAN**, na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE ou do dispositivo CPE.
   - Caso tenha atribuído uma função a um dispositivo CPE na seção **Tags de topologia**, clique em **Salvar**.

A função é atribuída ao dispositivo CPE.

Atribuir uma tag de topologia a um dispositivo CPE

É possível atribuir uma tag de topologia a um modelo de CPE ou a um dispositivo CPE. Uma tag de topologia atribuída a um modelo de CPE é automaticamente atribuída a todos os dispositivos CPE que usam o modelo. Os dispositivos CPE com as mesmas tags de topologia estabelecem links entre si automaticamente. Uma tag de topologia não pode ser atribuída a um dispositivo CPE se tiver sido atribuída a função de Gateway SD-WAN ao dispositivo CPE.

Para atribuir uma tag de topologia a um dispositivo CPE:

1. Atribua uma tag de topologia a um dispositivo CPE de uma das seguintes formas:

   - Para atribuir uma tag de topologia a um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Topologia**.
   - Para atribuir uma tag de topologia a um dispositivo CPE, execute uma das seguintes ações:
     - No menu, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE, selecione a guia **Topologia** e marque a caixa de seleção **Substituir**.
     - No menu, vá para a seção **Infraestrutura**, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador, vá para a seção **Tags de topologia** e, na lista suspensa **Switch**, selecione o dispositivo CPE.

   As tags de topologia são exibidas.

2. No campo **Tags de topologia**, insira a tag de topologia que deseja atribuir ao dispositivo CPE e clique no ícone adicionar +.

   A tag de topologia é atribuída ao dispositivo CPE. É possível atribuir várias tags de topologia ou remover uma tag de topologia. Para remover uma tag de topologia, clique no ícone remover ✕ ao lado dela.

3. Salve as tags de topologia do dispositivo CPE de uma das seguintes formas:

   - Caso tenha atribuído uma tag de topologia a um modelo de CPE ou a um dispositivo CPE na seção **SD-WAN**, na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE ou do dispositivo CPE.

   - Caso tenha atribuído uma tag de topologia a um dispositivo CPE na seção **Tags de topologia**, clique em **Salvar**.

Configurar caminhos

É possível configurar caminhos em um segmento, modelo de CPE ou no dispositivo CPE. As configurações de caminho especificadas em um segmento ou modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que pertencem ao segmento ou usam o modelo de CPE. As configurações de caminho especificadas em um dispositivo CPE são propagadas automaticamente para todos os dispositivos CPE que pertencem ao mesmo segmento daquele dispositivo CPE.

Para configurar caminhos:

1. Configure caminhos de uma das seguintes formas:

   - Para configurar caminhos em um segmento, vá para a seção **Infraestrutura** e clique **Gerenciamento** → **Configurações de implementação** ao lado do controlador; então, vá para a seção **Segmentos** e clique em **Gerenciamento** → **Editar** ao lado do segmento.

   - Para configurar caminhos em um modelo de CPE, vá para a seção **SD-WAN** → **Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Múltiplos caminhos**.

   - Para configurar caminhos em um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **Múltiplos caminhos**.

   As configurações de caminho são exibidas.

2. No campo **Número máximo de caminhos**, insira o número máximo de caminhos compatíveis com o segmento ou dispositivo CPE. Intervalo de valores: 1 a 16. O valor padrão é `8`.

3. No campo **Limite máximo de Auto-SPF**, insira o número máximo de caminhos Auto-SPF compatíveis com o segmento ou dispositivo CPE. Os caminhos Auto-SPF automáticos são calculados automaticamente pelo controlador. Intervalo de valores: 1 a 8. Valor padrão: `2`.

   Para que o tráfego seja transmitido entre dispositivos CPE no modo Ativo/Ativo, insira um valor maior que `1` nesse campo. Para que o tráfego seja transmitido entre dispositivos CPE no modo Ativo/Espera, insira `1` nesse campo.

4. No campo **Multiplicador de variação de custo**, insira o índice máximo do custo do caminho para o custo mais baixo de qualquer caminho em sua rede SD-WAN; se o custo do caminho estiver abaixo do limite, o caminho pode ser adicionado ao segmento. Intervalo de valores: 1,0 a 10,0. Valor padrão: `10`. Não é possível inserir um valor nesse campo se a caixa de seleção **Balanceamento ponderado** estiver marcada.

   Por exemplo, se você inserir `2` nesse campo e o custo de caminho mais baixo na rede SD-WAN for 10.000, caminhos com um custo de até 20.000 poderão ser adicionados ao segmento. No modo Ativo/Espera, o valor nesse campo determina qual caminho de Auto-SPF é usado se o caminho de Auto-SPF anterior se tornar indisponível.

5. Caso deseje que os caminhos sejam adicionados ao segmento independentemente do custo, marque a caixa de seleção **Balanceamento ponderado**. Esta caixa de seleção está desmarcada por padrão.

6. Caso esteja configurando caminhos em um segmento, adicione ou modifique caminhos TE manuais conforme necessário.

7. Salve as configurações de caminho de uma das seguintes formas:

   - Caso tenha configurado caminhos no segmento, clique em **Salvar** para salvar as configurações do segmento.

   - Caso tenha configurado caminhos em um modelo de CPE ou no dispositivo CPE:

     Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do dispositivo CPE ou agende um salvamento posterior clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

As configurações de caminho são salvas.

Gerenciar links

É possível visualizar os links de uma das seguintes maneiras:

- Para visualizar a tabela de links estabelecidos de um dispositivo CPE, vá para a seção **SD-WAN** → **CPE** do menu, clique no dispositivo CPE e selecione a guia **Links**.

- Para visualizar a tabela com todos os links, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Links**.

- Para visualizar a topologia gráfica com todos os links, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento**→ **Configurações de implementação** ao lado do controlador e vá para a seção **Topologia**.

As informações sobre os links são exibidas nas seguintes colunas da tabela de links:

- **Origem** é o nome, DPID e número da porta OpenFlow do dispositivo CPE que é a origem do link.

- **IP/porta de origem** é o endereço IP e a porta da origem do link, separados por dois pontos.

- **NAT/origem disjunta** é o atributo topológico da origem do link, responsável por enviar informações sobre as interfaces SD-WAN ao controlador. Valores possíveis:

  - **N** (Desativado. As informações da interface SD-WAN não são enviadas ao controlador).

  - **NAT/PAT** (a interface SD-WAN está atrás do NAT ou PAT).

  - **WAN disjunta** (a interface SD-WAN está conectada a uma rede isolada).

- **Destino** é o nome, DPID e número da porta OpenFlow do dispositivo CPE que é o destino do link.

- **IP/porta de destino** é o endereço IP e a porta do destino do link, separados por dois pontos.

- **NAT/destino disjunto** é o atributo topológico do destino do link, responsável por enviar informações sobre as interfaces SD-WAN ao controlador. Valores possíveis:

  - **N** (Desativado. As informações da interface SD-WAN não são enviadas ao controlador).
  - **NAT/PAT** (a interface SD-WAN está atrás do NAT ou PAT).
  - **WAN disjunta** (a interface SD-WAN está conectada a uma rede isolada).

  Se necessário, é possível ocultar todas as colunas, exceto **Origem**, **NAT/origem disjunta**, **IP/porta de origem**, **Destino**, **NAT/destino disjunto** e **IP/porta de destino** clicando no ícone de configurações e selecionando **Mostrar IPs de túnel** no menu.

- **Último recurso** indica se o controlador usa o link como o último recurso ao calcular o caminho, independentemente dos indicadores de monitoramento:

  - **Y**
  - **N**

- **Monitoramento de limite** determina se o monitoramento de limite nos links é usado. Valores possíveis:

  - **Y** (monitoramento ativado).
  - **N** (monitoramento desativado).

- **Criptografia** é o status de criptografia do link. Valores possíveis:

  - **Configurado**
  - **Ativado**
  - **Desativado**

- **CFM** é o intervalo de tempo para enviar pacotes de controle quando o Gerenciamento de falhas de conectividade está em execução. Essa coluna exibe dois valores no formato **<valor 1>/<valor 2>**:

  - **<valor 1>** é o intervalo de tempo para enviar pacotes de controle especificado ao ativar o CFM no dispositivo CPE.
  - **<valor 2>** é o intervalo de tempo para enviar pacotes de controle sendo usado no momento. Um dos seguintes intervalos pode ser usado para enviar pacotes de controle:

    - O intervalo de tempo para enviar pacotes de controle especificado ao ativar o CFM no dispositivo CPE. Caso sejam especificados intervalos de tempo diferentes para enviar pacotes de controle em dispositivos CPE, o maior intervalo será usado. Por exemplo, caso tenha sido especificado 300 milissegundos como intervalo do pacote de controle no CPE 1 e um segundo no CPE 2, o intervalo do pacote de controle é de 1 segundo.
    - O intervalo de tempo para enviar pacotes de controle especificado ao ativar o CFM no link. O intervalo de tempo para enviar pacotes de controle definido para o link substitui os intervalos para enviar pacotes de controle definidos em dispositivos CPE. Por exemplo, caso tenha especificado 300 milissegundos como o intervalo do pacote de controle no CPE 1, um segundo no CPE 2 e 10 segundos no link entre o CPE 1 e o CPE 2, o intervalo de tempo resultante é de 10 segundos.

  Os valores especificados manualmente nessa coluna ficam sublinhados.

- **MTU** é o valor de MTU do link.
- **Erros/segundo** é o número de erros por segundo no link.
- **Utilização (%)** é a carga do link em forma de uma porcentagem da largura de banda da interface de serviço de origem.
- **Latência (ms)** é o tempo de atraso em milissegundos para o tráfego transmitido através do link.
- **Jitter (ms)** é o tempo de jitter em milissegundos para o tráfego transmitido através do link.
- **Perda de pacotes (%)** é a porcentagem de perda de pacotes de tráfego no link.
- **Velocidade (Mbit/s)** é a velocidade da transmissão do tráfego através do link em Mbps.
- **Estado de configuração da FEC/Estado operacional da FEC** é o status de configuração/operacional da Correção de erros de encaminhamento na conexão (**Ativado** ou **Desativado**).
- **Custo** é o custo do link.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Visualizar estatísticas de um link

Para visualizar as estatísticas de um link:

1. Acesse as estatísticas do link de uma das seguintes formas:

   - Para visualizar as estatísticas de um link estabelecido a partir de um dispositivo CPE, vá para a seção **SD-WAN → CPE** do menu e clique no dispositivo CPE; na seção**Links**, clique no botão **Gerenciamento** do link relevante e selecione **Visualizar estatísticas**.
   - Para visualizar as estatísticas de um dos links na tabela com todos os links, vá para a seção **Infraestrutura** do menu, clique no botão **Gerenciamento** ao lado do controlador e selecione **Configurações de implementação**; então, na seção **Links**, clique no botão **Gerenciamento** do link relevante e selecione **Visualizar estatísticas**.
   - Para visualizar as estatísticas de um dos links na topologia gráfica com todos os links, vá para a seção **Infraestrutura** do menu, clique no botão **Gerenciamento** ao lado do controlador e selecione **Configurações de implementação**; então, na seção **Topologia**, clique no link e selecione **Visualizar estatísticas**.

   Isso abre a janela de estatísticas do link. As estatísticas são exibidas em várias tabelas nas guias correspondentes: **Telemetria de link**, **Criptografia**, CFM, FEC.

   Configuração eficaz

   Origem da configuração

   Switch

   Tipo

   Ativado

   Intervalo

   1s

Status operacional

Tipo

Ativado

Intervalo

1s

FEC

Configuração eficaz

Origem da configuração

Switch

Tipo

Desativado

Taxa de FEC

Tempo máximo no buffer de reorganização (ms)

Status operacional

Tipo

Desativado

Taxa de FEC

Tempo máximo no buffer de reorganização (ms)

Pacotes originais enviados

Pacotes FEC enviados

Taxa de FEC em pacotes (%)

Bytes originais enviados

Bytes FEC enviados

Taxa de FEC em bytes (%)

Taxa de transferência de pacotes originais (pacotes/s)

Taxa de transferência de pacotes totais (pacotes/s)

Taxa de transferência de dados originais (Kbps)

Taxa de transferência de dados completos (Kbps)

Porcentagem de pacotes originais perdidos (%)

Taxa de total de perda de pacotes (%)

Atualizar automaticamente o custo do link com base na taxa de dados máxima da interface

Se a taxa de dados da interface WAN do SD-WAN no dispositivo CPE for maior que a taxa de rede fornecida pelo ISP, limite a taxa máxima da interface para corresponder à taxa de rede.

Exemplo:
O provedor de serviços fornece ao cliente acesso à Internet a uma taxa de 50 Mbps, e a velocidade da conexão física na interface do dispositivo CPE é de 100 Mbps. Nesse caso, para calcular corretamente o custo do link e a QoS, especifique a taxa máxima de 50.

É possível especificar a taxa máxima ao criar ou modificar uma interface SD-WAN de saída que participa da conexão. O custo da conexão é calculado com base no menor valor da taxa máxima das interfaces nas duas extremidades da conexão. A relação entre os parâmetros de taxa máxima e custo é a seguinte:

- A taxa máxima especifica a largura de banda máxima da interface para o cálculo correto das filas lógicas de QoS. Medição em Mbps.
- O custo determina o peso da interface na topologia e é calculado usando a fórmula: `Custo = 10.000.000/Velocidade`, em que `Velocidade` é igual à taxa máxima. Quanto menor o valor do custo, maior a prioridade do link na topologia da rede.

Quando a taxa máxima é alterada, o valor do custo dos links em ambas as direções também é alterado. O menor valor de taxa máxima das interfaces que participam do link é usado para o cálculo do link.

Em vez de calcular automaticamente o custo da conexão, é possível definir o custo manualmente.

Especificar o custo de um link

Para especificar o custo de um link:

1. Especifique o custo do link de uma das seguintes formas:
   - Para especificar o custo de um link estabelecido a partir de um dispositivo CPE, vá para a seção **SD-WAN→ CPE**, clique no dispositivo CPE, selecione a guia **Links** e clique em **Gerenciamento→ Definir custo** ao lado do link.
   - Para especificar o custo de um dos links na tabela com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento→ Configurações de implementação** ao lado do controlador, vá para a seção **Links** e clique em **Gerenciamento→ Definir custo** ao lado do link.
   - Para especificar o custo de um dos links na topologia gráfica com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento→ Configurações de implementação** ao lado do controlador, vá para a seção **Topologia**, clique no link e, então, em **Definir custo**.
2. Na janela aberta, marque a caixa de seleção **Substituir** para especificar o custo do link. Esta caixa de seleção está desmarcada por padrão.
3. No campo **Custo de link**, insira o custo do link. Para especificar o mesmo custo para o link na direção oposta, marque a caixa de seleção **Salvar para ambos os links**. Esta caixa de seleção está desmarcada por padrão.
4. Clique em **Salvar**.

   O custo do link é especificado.
5. Caso tenha especificado o custo de um link estabelecido a partir do dispositivo CPE, clique em**Salvar** na parte superior da área de configurações para salvar as configurações do dispositivo CPE.

Ativar a atenuação

A *atenuação* é um mecanismo configurável que exclui links instáveis cujo estado muda com muita frequência do cálculo do caminho. Ao determinar a instabilidade do link, as seguintes alterações de estado são consideradas:

- PARA CIMA/ATIVO → PARA BAIXO/INATIVO.
- PARA BAIXO/INATIVO → PARA CIMA/ATIVO.
- PARA CIMA/ATIVO → PARA CIMA/INATIVO.
- PARA CIMA/INATIVO → PARA CIMA/ATIVO.

Quando a atenuação é ativada em um link, cada alteração de estado do link aumenta o valor da penalidade. Se a penalidade atingir o limite no tempo especificado, o acesso ao link é restrito (seu custo é aumentado 10.000 vezes durante o período especificado). O valor de cada um desses parâmetros é especificado ao ativar a atenuação. Por padrão, o acesso ao link é retomado se o estado do link não for alterado por 10 minutos.

Para ativar a atenuação:

1. Ative a atenuação de uma das seguintes formas:
   - Para ativar a atenuação de um link estabelecido a partir de um dispositivo CPE, vá para a seção **SD-WAN→ CPE**, clique no dispositivo CPE, selecione a guia **Links** e clique em **Gerenciamento** → **Atenuação** ao lado do link.
   - Para ativar a atenuação de um dos links na tabela com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador, vá para a seção **Links** e clique em **Gerenciamento** → **Atenuação** ao lado do link.
   - Para ativar a atenuação de um dos links na topologia gráfica com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador, vá para a seção **Topologia**, clique no link e, então, em **Atenuação**.
2. Na janela aberta, marque a caixa de seleção **Ativar** para ativar a atenuação no link. Esta caixa de seleção está desmarcada por padrão.
3. No campo **Tempo máximo de supressão (ms)**, insira o tempo, em milissegundos, durante o qual o acesso ao link pode ser restringido. Quando o tempo especificado expirar, todos os contadores de atenuação no link são redefinidos. O valor padrão é `600000`.
4. No campo **Penalidade**, insira em quanto a penalidade é incrementada quando o link muda de estado. O valor padrão é `1`.
5. No campo **Limite de supressão**, insira o valor da penalidade na qual o acesso ao link é restringido. O valor padrão é `4`.
6. No campo **Intervalo de atualização (ms)**, insira o tempo, em milissegundos, durante o qual a Penalidade deve atingir o valor especificado no campo **Limite de supressão** para que o acesso ao link seja restringido. O valor padrão é `120000`.
7. Para visualizar as estatísticas de atenuação de um link, clique em **Estatísticas de carga**.

8. Clique em **Salvar**.

   A atenuação é ativada no link.

9. Caso tenha ativado a atenuação em um link estabelecido a partir do dispositivo CPE, clique em **Salvar** na parte superior da área de configurações para salvar as configurações do dispositivo CPE.

Ativar a Correção de erros de encaminhamento

A funcionalidade de *Correção de erros de encaminhamento (FEC)* reduz a perda de pacotes de tráfego em links, especialmente para aplicativos UDP, e o número de retransmissões, que levam a atrasos, além de recuperar dados recebidos no dispositivo CPE. A recuperação de dados é fornecida pela codificação redundante do fluxo de dados no dispositivo CPE de origem.

Se a FEC estiver ativada em um link, o dispositivo CPE de origem codifica o fluxo de pacotes de tráfego transmitido através do link e adiciona pacotes de tráfego redundantes. A codificação em dispositivos CPE pode causar atrasos devido ao processamento extra de dados.

O dispositivo CPE de destino armazena em buffer os pacotes de tráfego recebidos através do link e os decodifica, recuperando os pacotes de tráfego perdidos, se possível. Recomendamos usar a FEC em links ruidosos para reduzir a perda de pacotes e aumentar a velocidade das conexões TCP. O diagrama geral de FEC é mostrado na figura abaixo.

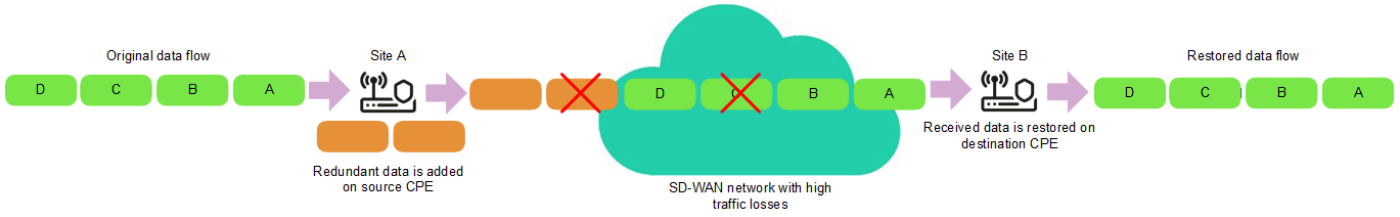


Diagrama de FEC

Para ativar a FEC:

1. Ative a FEC de uma das seguintes formas:

   - Para ativar a FEC de um link estabelecido a partir de um dispositivo CPE, vá para a seção **SD-WAN → CPE**, clique no dispositivo CPE, selecione a guia **Links** e clique em **Gerenciamento → FEC/reordenamento** ao lado do link.

   - Para ativar a FEC de um dos links na tabela com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador, vá para a seção **Links** e clique em **Gerenciamento → FEC/reordenamento** ao lado do link.

   - Para ativar a FEC de um dos links na topologia gráfica com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador, vá para a seção **Topologia**, clique no link e, então, em **FEC/reordenamento**.

   - Para ativar a funcionalidade FEC de um dos links ao criar uma interface SD-WAN do tipo WAN, vá para a seção **SD-WAN→ CPE** do menu, clique em um dispositivo CPE, selecione a guia **SD-WAN→ Interfaces** na tabela de interfaces SD-WAN, clique no botão **+ Adicionar** e selecione a guia **Configurações de link**.

2. Na janela aberta, ative o botão **Substituir** para substituir as configurações de link.

   Esse botão é desativado por padrão e não é exibido caso a FEC seja configurada ao criar uma interface SD-WAN do tipo WAN.

3. Ative a FEC para o link usando o botão **Ativar FEC**. Esse botão é desativado por padrão.

4. Na lista suspensa **Índice de redundância (pacote original/redundante)**, selecione o índice de pacotes de tráfego originais para pacotes de tráfego extra com código redundante. Valor padrão: **0:0 (FEC desativado)** significa que o FEC não é usado. Também é possível o índice de pacotes de tráfego originais para pacotes de tráfego redundantes usando a propriedade do controlador `topology.link.fec.ratio`.

5. No campo **Tempo limite de buffer de reordenação (ms)**, insira o tempo, em milissegundos, durante o qual um pacote de tráfego pode permanecer na fila para aplicação da FEC. Intervalo de valores: 1 a 1000.

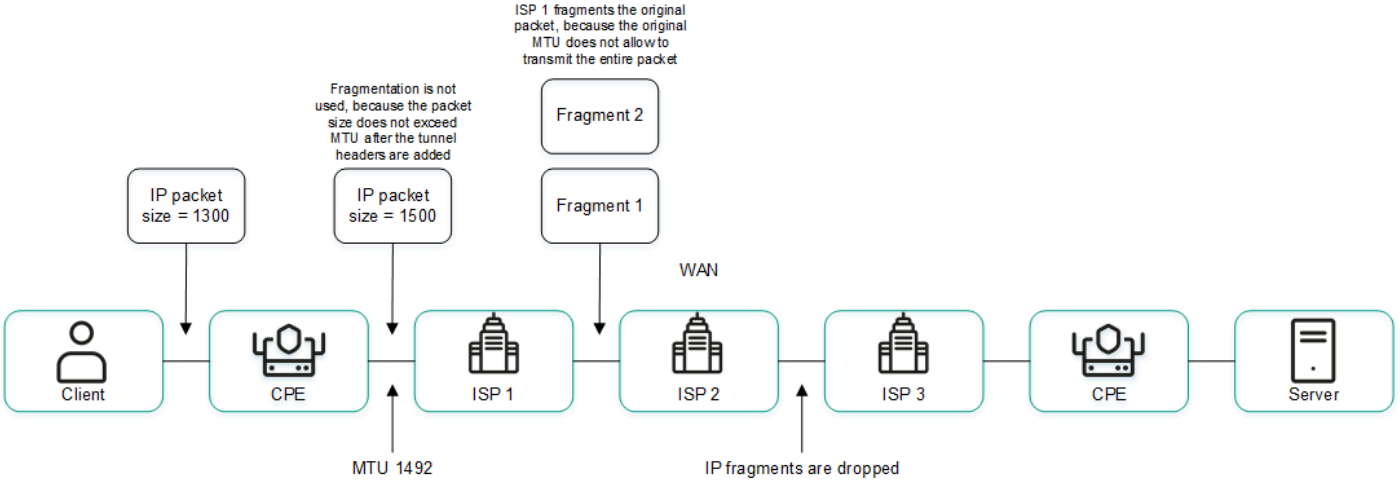
6. Clique em **Salvar**.

   A FEC é desativada.

7. Caso tenha ativado a FEC de um link estabelecido a partir do dispositivo CPE, clique em Salvar na parte superior da área de configurações para salvar as configurações do dispositivo CPE.

Determinar o valor de MTU

É possível determinar o valor de MTU de um link para descobrir por que os pacotes fragmentados estão sendo bloqueados no link (veja a figura abaixo).



Links com tamanho de MTU reduzido e pacotes fragmentados sendo descartados

O valor de MTU é determinado enviando pacotes LLDP com um tamanho de carga útil variável através do link. O tamanho mínimo detectável de MTU é 1280 bytes e o máximo é 1500 bytes. O valor de MTU é determinado automaticamente quando os dispositivos CPE são ativados e periodicamente em um intervalo especificado na propriedade do controlador `topology.link.pmtud.scheduler.interval.sec`.

É possível determinar o valor de MTU manualmente.

Para determinar o valor de MTU manualmente.

Determine o valor de MTU de uma das seguintes formas:

- Para determinar manualmente o valor de MTU de um link estabelecido a partir de um dispositivo CPE, vá para a seção **SD-WAN**→ **CPE**, clique no dispositivo CPE, selecione a guia **Links** e clique em **Gerenciamento** → **Verificar MTU** ao lado do link.
- Para determinar manualmente o valor de MTU em um dos links na tabela com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador, vá para a seção **Links** e clique em **Gerenciamento** → **Verificar MTU** ao lado do link.

O valor de MTU é exibido na coluna **MTU**.

Criptografia de tráfego

A *criptografia de tráfego* é um mecanismo para proteger a troca de tráfego entre dispositivos CPE por meio de links. Por exemplo, é possível criptografar o tráfego transmitido por links não seguros.

A criptografia de tráfego não substitui a necessidade de outras medidas de segurança da informação, como TLS, LDAPS e outros protocolos que protegem o tráfego na rede overlay.

O controlador gera automaticamente chaves para criptografar e descriptografar o tráfego e envia as chaves para os dispositivos CPE. O tráfego é criptografado no dispositivo CPE de origem usando a chave de criptografia. O dispositivo CPE de destino descriptografa o tráfego usando a chave de descriptografia.

As chaves são atualizadas regularmente para não permitir que terceiros criptografem ou descriptografem o tráfego transmitido se uma chave for interceptada. Especifique após quanto tempo as chaves são atualizadas nos dispositivos CPE usando a propriedade do controlador `topology.link.encryption.key.update.interval.minutes`.

A criptografia de tráfego é compatível apenas com dispositivos CPE que executam o software Kaspersky SD-WAN.

É possível ativar a criptografia de tráfego em um dispositivo CPE ou em um link. Um dispositivo CPE com a criptografia de tráfego ativada encaminha o tráfego criptografado em todos os seus links, incluindo novos links que serão estabelecidos no futuro. Quando a criptografia de tráfego é ativada em um link, o dispositivo CPE transmite o tráfego criptografado por esse link. Quando a criptografia de tráfego é desativada, as chaves geradas pelo controlador para criptografar e descriptografar o tráfego são excluídas de todos os dispositivos CPE conectados. Por padrão, a criptografia de tráfego é desativada em dispositivos CPE e links.

Por exemplo, é possível ativar a criptografia de tráfego em um dispositivo CPE e desativá-la em um dos links do dispositivo. Nesse caso, o dispositivo CPE transmite o tráfego criptografado por todos os seus links, exceto pelo link em que a criptografia de tráfego está desativada.

Ativar a criptografia de tráfego em um dispositivo CPE

Um dispositivo CPE com a criptografia de tráfego ativada encaminha o tráfego criptografado em todos os seus links, incluindo novos links que serão estabelecidos no futuro. É possível ativar ou desativar a criptografia de tráfego em um modelo de CPE ou em um dispositivo CPE. As configurações de criptografia de tráfego especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Para ativar a criptografia de tráfego em um dispositivo CPE:

1. Ative a criptografia de tráfego no dispositivo CPE de uma das seguintes formas:

   - Para ativar a criptografia de tráfego em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Criptografia de link**.

   - Para ativar a criptografia de tráfego em um dispositivo CPE, vá para a seção **SD-WAN→ CPE** do menu, clique no dispositivo CPE, selecione a guia **Criptografia de link** e marque a caixa de seleção **Substituir**.

   A política de criptografia de tráfego é exibida.

2. Na lista suspensa **Ativar a criptografia**, selecione **Ativado**. O valor padrão é **Desativado**.

3. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Ativar a criptografia de tráfego em um link

Quando a criptografia de tráfego é ativada em um link, o dispositivo CPE transmite o tráfego criptografado por esse link.

Para ativar a criptografia de tráfego em um link:

1. Ative a criptografia de tráfego no link de uma das seguintes formas:

   - Para ativar a criptografia de tráfego de um link estabelecido a partir de um dispositivo CPE, vá para a seção **SD-WAN→ CPE**, clique no dispositivo CPE, selecione a guia **Links** e clique em **Gerenciamento → Definir criptografia** ao lado do link.

   - Para ativar a criptografia de tráfego de um dos links na tabela com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador, vá para a seção **Links** e clique em **Gerenciamento → Definir criptografia** ao lado do link.

   - Para ativar a criptografia de tráfego de um dos links na topologia gráfica com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador, vá para a seção **Topologia**, clique no link e, então, em **Definir criptografia**.

2. Na janela aberta, marque a caixa de seleção **Substituir**. Esta caixa de seleção está desmarcada por padrão.

3. Marque a caixa de seleção **Ativar a criptografia** para ativar a criptografia de tráfego no link. Esta caixa de seleção está desmarcada por padrão.

4. Clique em **Salvar**.

   A criptografia de tráfego é ativada no link.

5. Caso tenha ativado a criptografia de tráfego em um link estabelecido a partir do dispositivo CPE, clique em **Salvar** na parte superior da área de configurações para salvar as configurações do dispositivo CPE.

Gerenciamento de falhas de conectividade (CFM)

A funcionalidade de *Gerenciamento de falhas de conectividade* (doravante também CFM) permite detectar links indisponíveis entre dispositivos CPE. Quando o CFM está ativado, o dispositivo CPE envia pacotes de controle de Mensagem de Verificação de Continuidade (CCM) por meio de seus links nos intervalos especificados e monitora os pacotes de controle de resposta nos links de direção oposta. Se os pacotes de controle de resposta não chegarem, o dispositivo CPE considera o link indisponível e inicia a transmissão do tráfego por meio de um link disponível selecionado aleatoriamente.

O tempo limite de resposta é igual ao intervalo de envio do pacote de controle vezes 3,5. O tempo necessário para passar um dispositivo CPE para uma nova conexão quando nenhum pacote de resposta é recebido é igual ao intervalo de envio do pacote de controle multiplicado por um número no intervalo de 3,5 a 7. Por exemplo, caso tenha sido especificado 300 milissegundos como o intervalo para o envio de pacotes de controle, o tempo limite de resposta é de 1,05 segundos e o tempo necessário para passar o dispositivo CPE para um novo link é de 1,05 a 2,1 segundos.

Ao usar o mecanismo CFM, recomendamos configurar o intervalo CFM e a propriedade do controlador `core.link.liveness.timeout` de forma que `core.link.liveness.timeout` >= intervalo CFM * 10.

É possível ativar o CFM em um dispositivo CPE ou um link:

- Um dispositivo CPE com CFM ativado envia pacotes de controle por todos os seus links, incluindo novos links estabelecidos no futuro. Caso sejam especificados intervalos de tempo diferentes para enviar pacotes de controle em dispositivos CPE, o maior intervalo será usado. Por exemplo, caso tenha sido especificado 300 milissegundos como intervalo do pacote de controle no CPE 1 e um segundo no CPE 2, o intervalo do pacote de controle é de 1 segundo.

  Quando o CFM é ativado em um dispositivo CPE e desativado no outro dispositivo CPE, o dispositivo CPE com o CFM ativado tem precedência. Nesse caso, os dispositivos CPE enviam pacotes de controle entre si por meio de todos os seus links.

- Quando o CFM é ativado para um link, o dispositivo CPE envia pacotes de controle somente por esse link. Ao ativar o CFM para um link, ative também o CFM no link de direção oposta. O intervalo de tempo para enviar pacotes de controle definido para o link substitui os intervalos para enviar pacotes de controle definidos em dispositivos CPE. Por exemplo, caso tenha especificado 300 milissegundos como o intervalo do pacote de controle no CPE 1, um segundo no CPE 2 e dez segundos no link entre o CPE 1 e o CPE 2, o intervalo de tempo resultante é de dez segundos.

Por exemplo, é possível ativar o CFM em um dispositivo CPE e desativá-lo em um dos links do dispositivo. Nesse caso, o dispositivo CPE envia pacotes de controle por todos os seus links, exceto pelo link em que o CFM está desativado. Por padrão, o CFM é desativado em dispositivos CPE e links.

Alterar as configurações de CFM em uma conexão ativa pode causar interrupções no tráfego.

Ativar o CFM em um dispositivo CPE

Um dispositivo CPE com CFM ativado envia pacotes de controle por todos os seus links, incluindo novos links estabelecidos no futuro. É possível ativar ou desativar o CFM em um modelo de CPE ou em um dispositivo CPE. As configurações de CFM especificadas no modelo de CPE são propagadas automaticamente para todos os dispositivos CPE que usam o modelo.

Quando o CFM é ativado em um dispositivo CPE e desativado no outro dispositivo CPE, o dispositivo CPE com o CFM ativado tem precedência. Nesse caso, os dispositivos CPE enviam pacotes de controle entre si por meio de todos os seus links.

Alterar as configurações de CFM em uma conexão ativa pode causar interrupções no tráfego.

Para ativar o CFM em um dispositivo CPE:

1. Ative o CFM no dispositivo CPE de uma das seguintes formas:

   - Para ativar o CFM em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **CFM**.

   - Para ativar o CFM em um dispositivo CPE, vá para a seção **SD-WAN→ CPE** do menu, clique no dispositivo CPE, selecione a guia **CFM** e marque a caixa de seleção **Substituir**.

2. Na lista suspensa **CFM**, selecione **Ativado**. O valor padrão é **Desativado**.

3. Na lista suspensa **Intervalo**, selecione o intervalo de tempo para o envio de pacotes de controle:

   - **300 ms**.

   - **1 s**. Essa é a configuração padrão.

   - **10 s**.

   - **1 min**.

   O tempo limite de resposta é igual ao intervalo de envio do pacote de controle vezes 3,5. O tempo necessário para passar um dispositivo CPE para uma nova conexão quando nenhum pacote de resposta é recebido é igual ao intervalo de envio do pacote de controle multiplicado por um número no intervalo de 3,5 a 7. Por exemplo, caso tenha selecionado **300 ms** na lista suspensa **Intervalo**, o tempo limite de resposta é de 1,05 segundos e o tempo necessário para passar o dispositivo CPE para um novo link é de 1,05 a 2,1 segundos.

   Caso tenha especificado intervalos diferentes de pacotes de controle em dispositivos CPE, o maior dos intervalos especificados é usado. Por exemplo, se na lista suspensa **Intervalo** para o CPE 1, tenha sido selecionado **300 ms** e **1 s** para o CPE 2, o intervalo de tempo para o envio de pacotes de controle é de 1 segundo.

4. Na parte inferior da área de configuração, clique no botão **Salvar** para salvar imediatamente as configurações do modelo de CPE ou dispositivo CPE, ou agende um salvamento posterior das configurações do dispositivo CPE clicando no ícone ⌄ à direita do botão **Salvar** e selecionando a opção **Programação salva**.

Ativar o CFM em um link

Quando o CFM é ativado para um link, o dispositivo CPE envia pacotes de controle somente por esse link. Ao ativar o CFM para um link, ative também o CFM no link de direção oposta.

Alterar as configurações de CFM em uma conexão ativa pode causar interrupções no tráfego.

Para ativar o CFM em um link:

1. Ative o CFM no link de uma das seguintes formas:

   - Para ativar o CFM em um link estabelecido a partir de um dispositivo CPE, vá para a seção **SD-WAN→ CPE**, clique no dispositivo CPE, selecione a guia **Links** e clique em **Gerenciamento → Definir CFM** ao lado do link.

   - Para ativar o CFM de um dos links na tabela com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador, vá para a seção **Links** e clique em **Gerenciamento → Definir CFM** ao lado do link.

2. Para ativar o CFM de um dos links na topologia gráfica com todos os links, vá para a seção **Infraestrutura**, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador, vá para a seção **Topologia**, clique no link e, então, em **Definir CFM**.

3. Na janela aberta, marque a caixa de seleção **Substituir**. Esta caixa de seleção está desmarcada por padrão.

4. Selecione **Salvar para ambos os links** para ativar o CFM no link na direção oposta. Esta caixa de seleção está desmarcada por padrão.

5. Na lista suspensa **CFM**, selecione **Ativado**. O valor padrão é **Desativado**.

6. Na lista suspensa **Intervalo**, selecione o intervalo de tempo para o envio de pacotes de controle:

   - **300 ms**.

   - **1 s**. Essa é a configuração padrão.

   - **10 s**.

   - **1 min**.

   O tempo limite de resposta é igual ao intervalo de envio do pacote de controle vezes 3,5. O tempo necessário para passar um dispositivo CPE para uma nova conexão quando nenhum pacote de resposta é recebido é igual ao intervalo de envio do pacote de controle multiplicado por um número no intervalo de 3,5 a 7. Por exemplo, caso tenha selecionado **300 ms** na lista suspensa **Intervalo**, o tempo limite de resposta é de 1,05 segundos e o tempo necessário para passar o dispositivo CPE para um novo link é de 1,05 a 2,1 segundos.

   O intervalo de tempo para o envio de pacotes de controle definido para o link substitui os intervalos para o envio de pacotes especificados ao ativar o CFM em dispositivos CPE. Por exemplo, caso na lista suspensa **Intervalo**, você tenha selecionado **300 ms** para o CPE 1, **1 s** para o CPE 2 e **10 s** para o link entre o CPE 1 e o CPE 2, o intervalo de tempo resultante para o envio de pacotes de controle é de 10 segundos.

7. Clique em **Salvar**.

   O CFM é ativado para o link.

8. Caso tenha ativado o CFM em um link estabelecido a partir do dispositivo CPE, clique em **Salvar** na parte superior da área de configurações para salvar as configurações do dispositivo CPE.

Gerenciar segmentos

Para visualizar a tabela de segmentos, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Segmentos**. As informações sobre segmentos e os caminhos que eles contêm são exibidas nas seguintes colunas da tabela:

- **De** é o nome e DPID do dispositivo CPE da origem do segmento.
- **Para** é o nome e DPID do dispositivo CPE do destino do segmento.
- **Caminhos/máximo** é o número de caminhos criados e o número máximo de caminhos suportados pelo segmento.
- **#** é o número sequencial do caminho. Quanto menor o número do caminho, há mais tempo ele foi criado.
- **Tipo de caminho** é o tipo de evento.
  - **SPF automático**
  - **TE automático**
  - **TE manual**
- **Caminhos** são os nomes, DPIDs e números de portas OpenFlow de dispositivos CPE pelos quais o caminho passa.
- **Estado administrativo** é o estado administrativo do caminho:
  - **para cima**
  - **para baixo**
- **Estado operacional** é o estado operacional do caminho:
  - **para cima**
  - **para baixo**
- **Custo** é o custo do caminho.
- **Contagem de saltos** é o número de saltos no caminho.
- **Peso de balanceamento** é o peso do caminho calculado com base no custo total dos links.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um caminho de Manual-TE

Ao criar um caminho de Manual-TE, é necessário especificar manualmente os links pelos quais o caminho passa no trajeto do dispositivo CPE de origem do segmento para o dispositivo CPE de destino do segmento. Há suporte para dois tipos de caminhos de Manual-TE:

- Um *caminho de Manual-TE totalmente definido* especifica cada dispositivo CPE e interface de serviço pelo qual o caminho de Manual-TE passa.

- Um *caminho de Manual-TE híbrido* especifica um ou mais dispositivos CPE e interfaces de serviço pelos quais o caminho de Manual-TE passa. Nesse caso, o tráfego entre as seções do caminho de Manual-TE que não são especificadas manualmente é transmitido automaticamente (usando um caminho de Auto-SPF).

É possível usar restrições de Manual-TE para adicionar caminhos de Manual-TE aos serviços de transporte.

Exemplos de possíveis caminhos de Manual-TE:
Nos exemplos, um número de porta OpenFlow é especificado após o número do dispositivo CPE, separado por dois pontos.

Caminho de Manual-TE totalmente definido: CPE 1:3 → CPE 2:1, CPE 2:2 → CPE 4:1, CPE 4:5 → CPE N:2.

Caminho de Manual-TE híbrido: CPE 1 → CPE 5, CPE 5:3 → CPE 4:3, CPE 4 → CPE N. Nesse caso, o caminho do CPE 1 para o CPE N é criado como um caminho de Auto-SPF CPE 1 → CPE 5, um caminho de Manual-TE CPE 5:3 → CPE 4:3 e um caminho de Auto-SPF CPE 4 → CPE N.

Para criar um caminho de Manual-TE:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Segmentos**.

   Uma tabela de segmentos é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do segmento no qual deseja criar um caminho de Manual-TE.

   As configurações e a tabela de caminhos são exibidas.

   As informações sobre caminhos são exibidas nas seguintes colunas da tabela:

   - **Tipo de caminho** é o tipo de evento.

     - **SPF automático**

     - **TE automático**

     - **TE manual**

- **Estado administrativo** é o estado administrativo do caminho:
  - **para cima**
  - **para baixo**
- **Estado operacional** é o estado operacional do caminho:
  - **para cima**
  - **para baixo**
- **Custo** é o custo do caminho.
- **Contagem de saltos** é o número de saltos no caminho.
- **Balanceamento de carga** indica se o balanceamento de carga está ativado para o caminho.
- **Peso de balanceamento** é o peso do caminho para balanceamento, calculado com base no custo total dos links.

5. Clique em **+ Caminho de TE manual**.

   As configurações do caminho de Manual-TE e a tabela de saltos são exibidas.

   As informações sobre saltos são exibidas nas seguintes colunas da tabela:

   - **#** é o número sequencial do salto. Quanto menor o número do salto, há mais tempo ele foi adicionado.
   - **De** é o nome, DPID e número da porta OpenFlow do dispositivo CPE que é a origem do salto.
   - **Para** é o nome, DPID e número da porta OpenFlow do dispositivo CPE que é o destino do salto.
   - **Custo** é o custo do salto.

   O custo total do caminho de Manual-TE é exibido na parte superior da tabela.

6. No campo **Nome** da área de configurações, insira o nome do caminho de Manual-TE.

7. No campo **Número máximo de saltos**, insira o número máximo de saltos no caminho de Manual-TE. Intervalo de valores: 1 a 8. Valor padrão: 4.

8. Adicione o salto ao caminho de Manual-TE:

   a. Na lista suspensa **De** à esquerda, selecione o dispositivo CPE de origem para o salto.

      Caso esteja adicionando o primeiro salto ao caminho de Manual-TE, só é possível selecionar o dispositivo CPE da origem do segmento como dispositivo CPE de origem do salto. Caso tenha adicionado pelo menos um salto ao caminho de Manual-TE, só é possível selecionar o dispositivo CPE de destino do salto anterior como o dispositivo CPE de origem do salto atual.

   b. Se necessário, na lista suspensa **Porta** à esquerda, selecione a porta OpenFlow da origem do salto. Valor padrão: **Automaticamente** significa que a porta OpenFlow é determinada automaticamente.

   c. Na lista suspensa **Para** à direita, selecione o dispositivo CPE no final do salto.

Caso, na lista suspensa **Porta**, tenha sido selecionado **Automaticamente** como o dispositivo CPE de origem do salto, é possível selecionar qualquer dispositivo CPE que não esteja sendo usado em outros saltos como o destino do salto. Nesse caso, na lista suspensa **Porta**, **Automaticamente** é selecionado para o dispositivo CPE de destino do salto e a porta OpenFlow é detectada automaticamente. Assim, o salto usa um caminho de Auto-SPF.

Caso tenha selecionado uma porta OpenFlow para o dispositivo CPE de origem do salto na lista suspensa **Porta**, para o dispositivo CPE de destino do salto, só será possível usar um dispositivo CPE que tenha um link criado a partir dessa porta OpenFlow. Nesse caso, na lista suspensa **Porta**, a porta OpenFlow para a qual o link é criado é automaticamente selecionada como o dispositivo CPE de destino do salto. Assim, o salto usa o link especificado entre os dois dispositivos CPE.

d. Se necessário, na lista suspensa **Porta** à direita, selecione a porta OpenFlow do dispositivo CPE de destino do salto. Valor padrão: **Automaticamente** significa que a porta OpenFlow é determinada automaticamente.

e. Clique em **Adicionar**.

O salto é criado e exibido na tabela. É possível adicionar vários saltos ou excluir saltos. Para excluir um salto, selecione-o na tabela e clique no botão **Excluir**.

9. Clique em **Criar**.

Uma verificação é executada para garantir que o dispositivo CPE de destino do último salto corresponda ao dispositivo CPE de destino do segmento em que o caminho de Manual-TE está sendo criado. Se a verificação for bem-sucedida, o caminho de Manual-TE é criado e exibido na tabela e a coluna **Custo** exibe o custo do caminho de Manual-TE, que é a soma total do custo de todos os saltos adicionados a esse caminho de Manual-TE.

10. Clique em **Salvar** para salvar as configurações do segmento.

Editar um caminho de Manual-TE

Para editar um caminho de Manual-TE:

1. No menu, acesse a seção **Infraestrutura**.

A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Segmentos**.

Uma tabela de segmentos é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do segmento no qual deseja editar um caminho de Manual-TE.

As configurações e a tabela de caminhos são exibidas.

5. Clique em **Editar** ao lado do caminho de Manual-TE que deseja editar.

As configurações do caminho de Manual-TE e a tabela de saltos são exibidas.

6. Se necessário, edite as configurações do caminho de Manual-TE. Para obter uma descrição das configurações, consulte as instruções para criar um caminho de Manual-TE.

7. Clique em **Salvar**.

   O caminho de Manual-TE é modificado e atualizado na tabela.

8. Clique em **Salvar** para salvar as configurações do segmento.

Excluir um caminho de Manual-TE

Os caminhos Manual-TE excluídos não podem ser restaurados.

Para excluir um caminho de Manual-TE:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Segmentos**.

   Uma tabela de segmentos é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do segmento do qual deseja excluir um caminho de Manual-TE.

   As configurações e a tabela de caminhos são exibidas.

5. Clique em **Excluir** ao lado do caminho de Manual-TE que deseja excluir.

   O caminho de Manual-TE é excluído e não é mais exibido na tabela.

6. Clique em **Salvar** para salvar as configurações do segmento.

Qualidade de serviço (QoS)

Uma política de *Qualidade de serviço* (QoS) garante a transferência de dados de acordo com os requisitos definidos para as *classes de tráfego*. No Kaspersky SD-WAN, os seguintes componentes contribuem para a qualidade de serviço:

- Classes de tráfego - indicam a prioridade do processamento de tráfego e distribuem o tráfego entre as filas. Por exemplo, é possível usar uma das classes de tráfego para tráfego em tempo real que requer minimizar a perda de pacotes. O mapeamento do tráfego para classes de tráfego pode ser feito ao criar ou editar um classificador de tráfego.

- Classificadores de tráfego determinam se os valores DSCP especificados nos campos de cabeçalho do pacote de tráfego devem ou não ser confiáveis. Se um classificador de tráfego não confiar nos valores DSCP, ele os mapeia para as classes de tráfego. Especifique um classificador de tráfego ao criar ou editar uma regra de qualidade de serviço para fazer com que a regra de qualidade de serviço use esse classificador de tráfego.

- As regras de qualidade de serviço determinam se a largura de banda do tráfego processado pelos classificadores de tráfego é limitada. Especifique uma regra de qualidade de serviço ao criar ou editar um serviço de transporte para fazer com que o serviço de transporte use essa regra.

- As *restrições* são usadas para configurar como os caminhos são criados nos serviços de transporte. É possível criar dois tipos de restrições:

  - As restrições de Manual-TE adicionam caminhos de Manual-TE aos serviços de transporte.

  - As restrições de limite especificam os limites de monitoramento de link usados para criar caminhos de Auto-TE nos serviços de transporte.

  É possível especificar uma restrição ao criar ou editar um serviço de transporte para que o serviço de transporte use essa restrição.

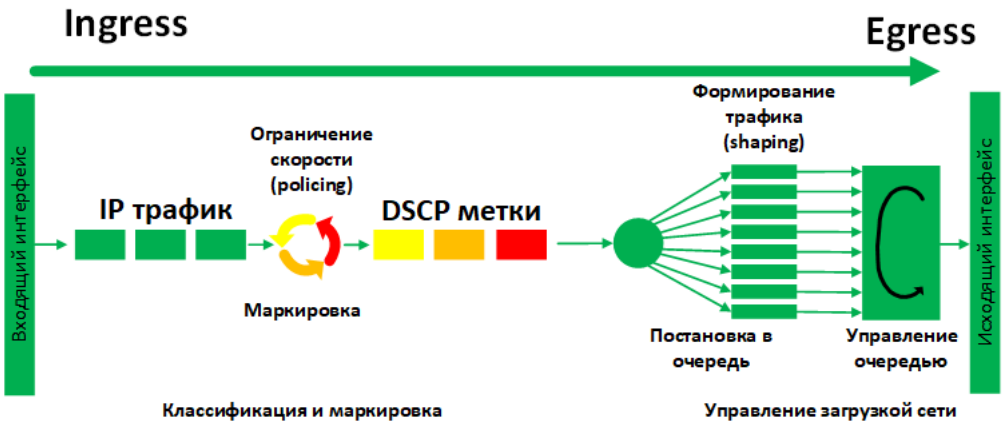
- As regras de classificação de tráfego identificam tráfego com valores específicos nos campos de cabeçalho L2 – L4, bem como tráfego de aplicativos especificados, no fluxo geral de tráfego. É possível especificar uma regra de classificação de tráfego ao criar ou editar um filtro de tráfego para que ele use essa regra.

- Os filtros de tráfego filtram o tráfego com base nas regras de classificação de tráfego especificadas. É possível especificar um filtro de tráfego ao criar ou editar um serviço de transporte ou uma interface ACL para que o serviço de transporte ou a interface ACL usem esse filtro de tráfego.

Mecanismos de qualidade de serviço

Uma política de QoS permite classificar e gerenciar as prioridades do processamento do tráfego de trânsito entre quaisquer interfaces CPE, incluindo interfaces de ponte, interfaces SD-WAN e serviços de transporte.

Um diagrama da aplicação de ferramentas de qualidade de serviço é mostrado na seguinte figura.



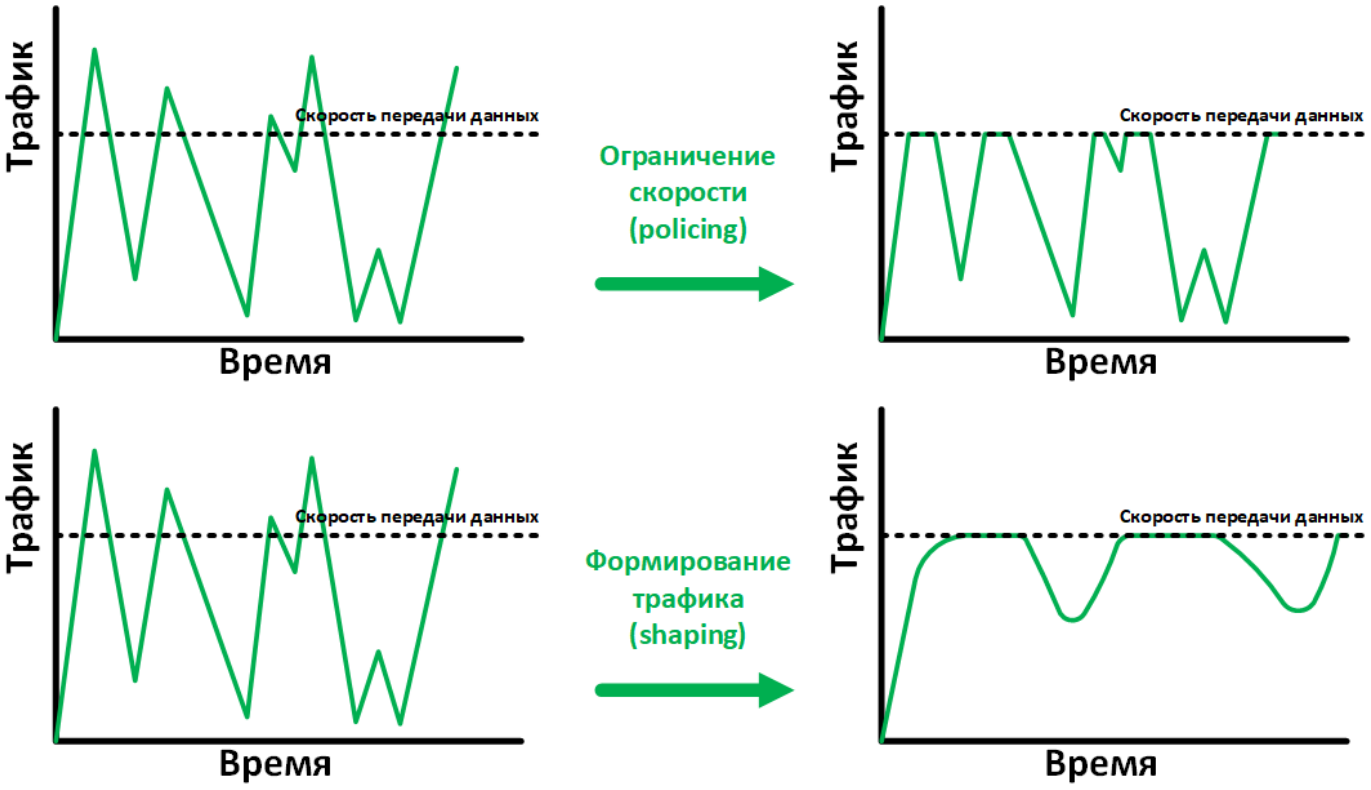
Ferramentas de QoS da solução SD-WAN

O tráfego que entra na interface de entrada pode ser marcado com base em vários atributos para corresponder às classes de tráfego predefinidas. Isso também pode alterar a marcação atualmente existente do tráfego de entrada.

Um mecanismo de limitação de taxa (*policiamento*) pode ser aplicado ao tráfego de entrada marcado de acordo com as classes de tráfego.

A *modelagem* de tráfego pode ser aplicada ao tráfego de saída marcado de acordo com as classes de tráfego.

O princípio de operação de policiamento e modelagem é mostrado na figura abaixo. O policiamento descarta o tráfego que excede o limite da taxa de dados. A modelagem suaviza a sobrecarga de tráfego ao introduzir um atraso adicional.



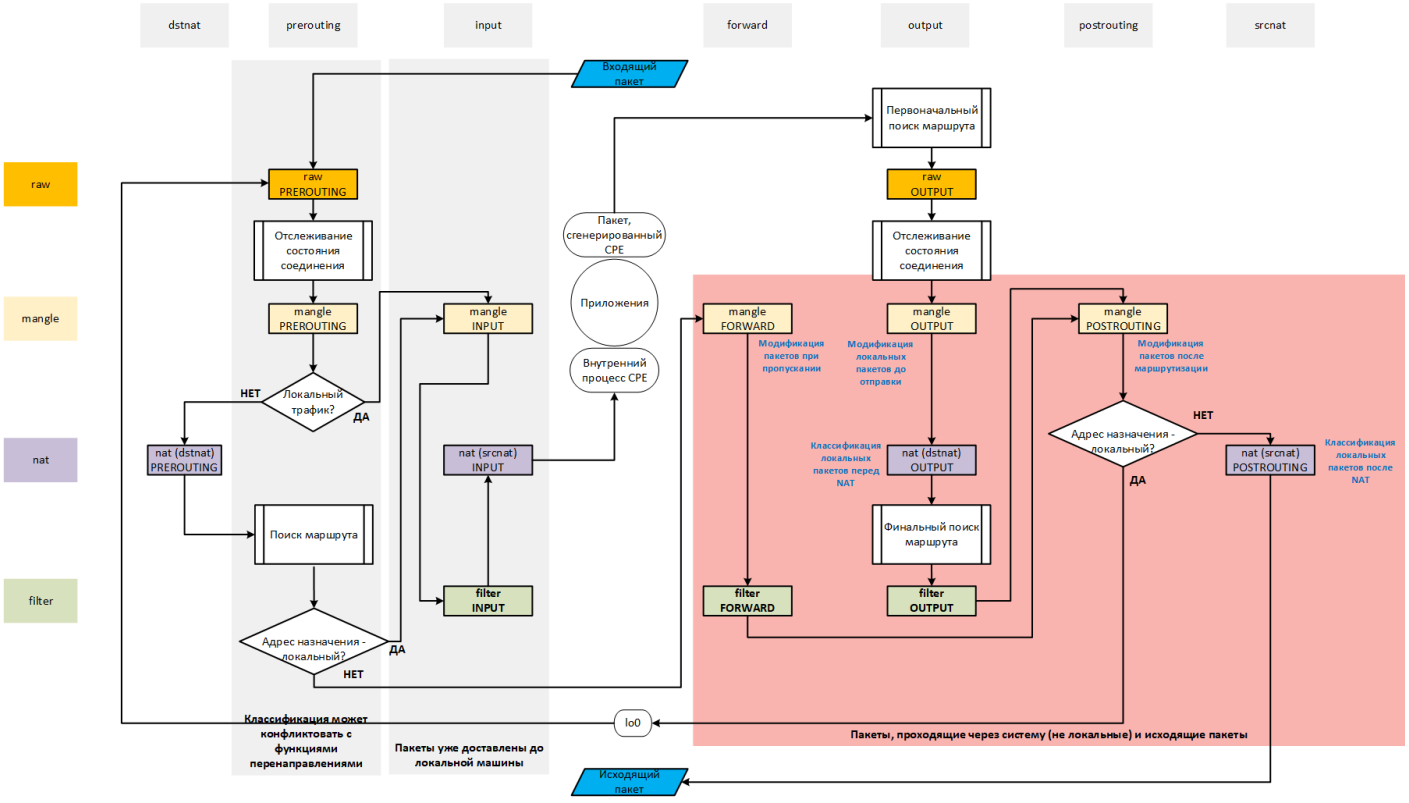
Mecanismos de processamento de tráfego

Marcação e remarcação de tráfego

Marcar usando CLASSIFY

Para mapear o tráfego de aplicativos para classes de tráfego adequadas para processamento adicional por mecanismos de QoS, você pode usar a funcionalidade CLASSIFY das regras de firewall avançadas.

O diagrama abaixo mostra como o tráfego é processado pelo firewall no formato clássico de filtro de pacotes iptables. A funcionalidade CLASSIFY está disponível em várias tabelas e cadeias.



Pontos de classificação (CLASSIFY) de regras de firewall avançadas

Para tráfego de trânsito, recomendamos usar a tabela MANGLE, a cadeia FORWARD.

É possível criar uma regra avançada que identifica algum tipo de tráfego de acordo com vários critérios na tabela MANGLE, na cadeia FORWARD e na ação CLASSIFY, e mapear esse tráfego para um número de fila.

> Você pode selecionar somente as filas de 0 a 6, que correspondem às classes de tráfego: *Melhor esforço*, *Negócio normal*, *Negócio crítico*, *Vídeo*, *Conferência*, *Sinalização*, *Tempo real*. Não é possível colocar o tráfego do aplicativo na fila 7 (a classe *Controle de rede*).

O tráfego marcado dessa forma é colocado diretamente na fila de saída. A marcação de tráfego é totalmente local e é usada somente dentro do dispositivo CPE para distribuir o tráfego às filas.

Marcação por meio de TOS

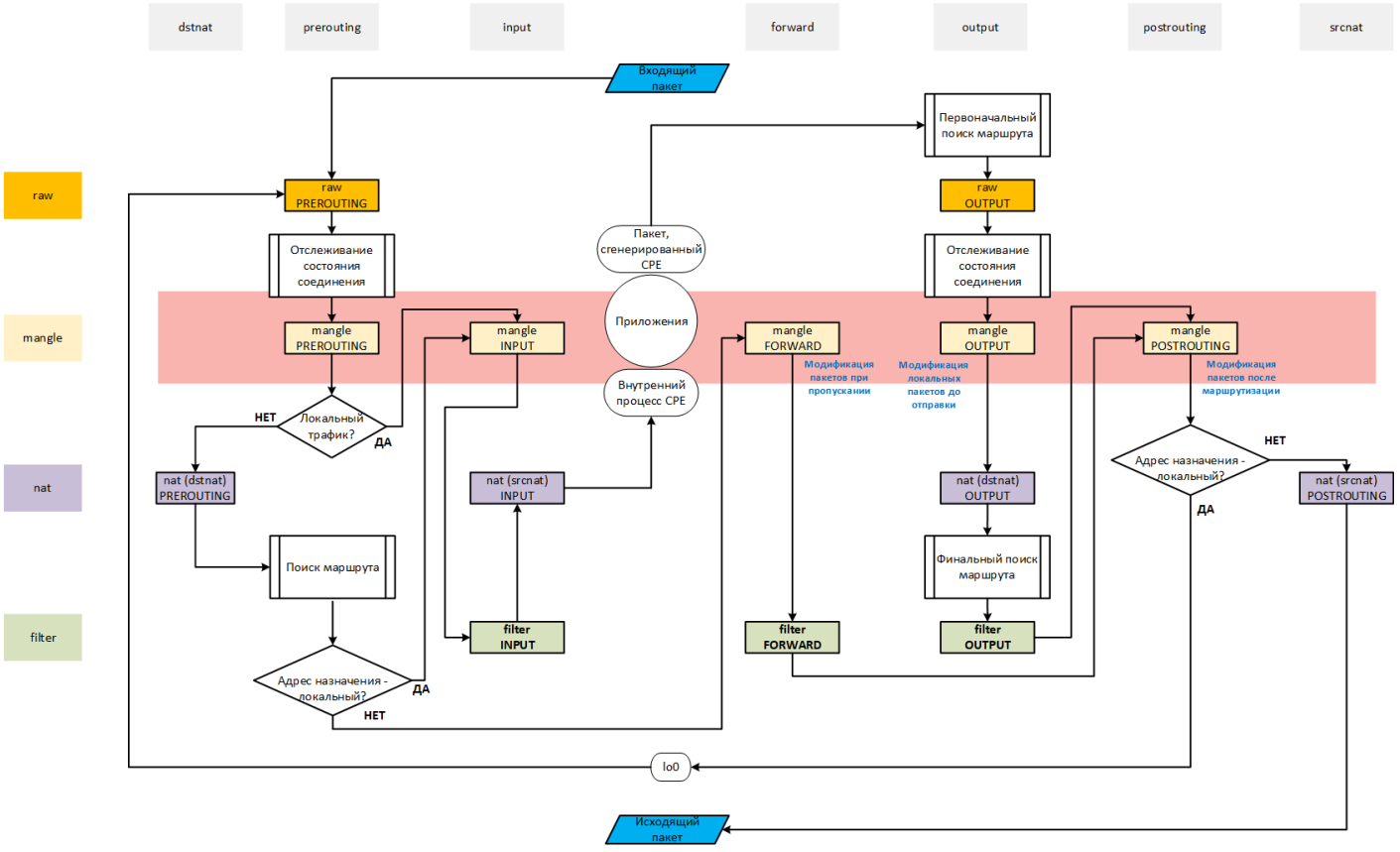
É possível marcar ou marcar novamente o tráfego de entrada para compará-lo com as classes de tráfego configuradas usando a ação TOS das regras avançadas de firewall.

Ao contrário da marcação CLASSIFY, os valores TOS/DSCP fazem parte do cabeçalho IP, o que significa que são visíveis fora do dispositivo e podem afetar o roteamento e a prioridade nas redes.

A tabela abaixo mostra a correspondência das marcas DSCP e TOS com classes de tráfego configuradas previamente.

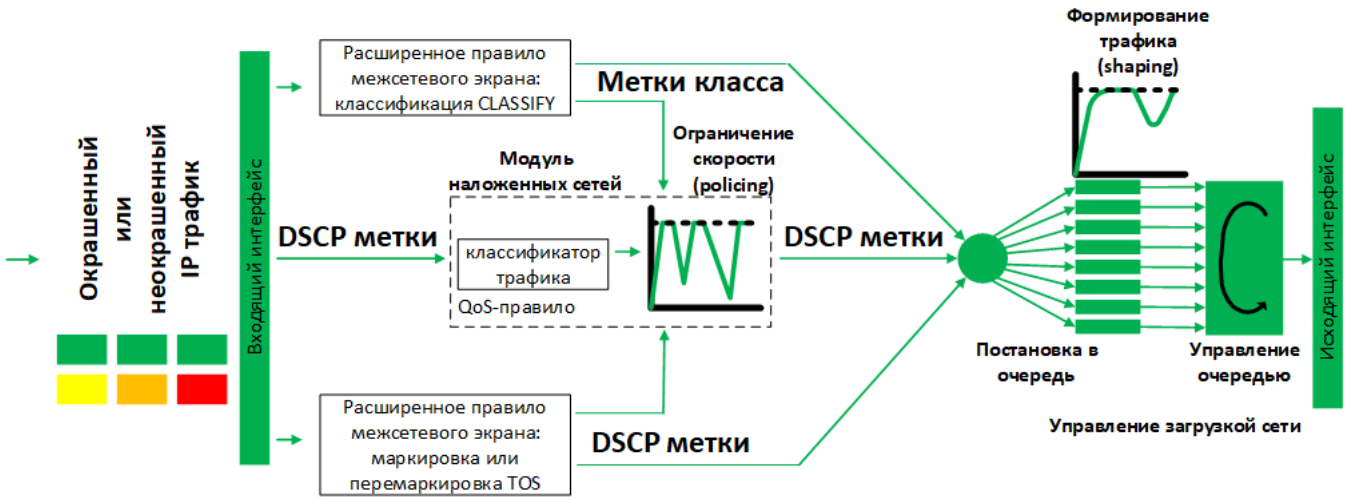
Correspondência de marcas DSCP e TOS com classes de tráfego configuradas previamente

Tag da classe de tráfego	Fila	Marcação DSCP	Marcação TOS
0	Melhor esforço	BE	0
1	Normal para o negócio	CS1	32
2	Crítico para o negócio	CS2	64
3	Sinalização	AF21	72
4	Vídeo	AF42	144
5	Conferência	EF	184
6	Tempo real	AF22	80



Pontos de marcação (TOS) de regras de firewall avançadas

O diagrama detalhado a seguir mostra como o aplicativo aplica os mecanismos de QoS SD-WAN da Kaspersky considerando redes de sobreposição.



Ferramentas de QoS da Kaspersky SD-WAN

Modelagem de tráfego

É possível configurar a modelagem de tráfego de acordo com as marcas de classe ou marcas DSCP nas interfaces de rede físicas ou lógicas do dispositivo CPE. A modelagem de tráfego é ativada separadamente para cada interface de rede individual. Para interfaces SD-WAN, essa função estará sempre ativada e será possível definir as configurações de modelagem de tráfego individuais.

Para configurar a modelagem de tráfego em interfaces de rede:

1. Configure a modelagem de tráfego de rede nas interfaces de rede por meio de uma das seguintes formas:

   - Caso queira configurar a modelagem de tráfego de rede em interfaces de rede em um modelo de CPE, acesse a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Rede**.

   - Caso queira configurar a modelagem de tráfego de rede em interfaces de rede em um dispositivo CPE, acesse a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **Rede**. Para editar uma interface de rede herdada do modelo de CPE, marque a caixa de seleção **Substituir** ao lado da interface de rede.

2. Selecione a interface de rede que deseja editar e clique no botão **Editar**.

3. Selecione a guia **QoS**.

4. Ative o botão de alternância **Ativado**.

5. Caso necessário, altere a taxa máxima total na interface e as configurações de largura de banda mínima e máxima para cada fila de tráfego.

6. Salve as alterações.

Para configurar a modelagem de tráfego em interfaces SD-WAN:

1. Prossiga com a configuração da modelagem de tráfego por meio de uma das seguintes formas:

   - Caso queira configurar a modelagem de tráfego nas interfaces SD-WAN em um modelo de CPE, acesse a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **SD-WAN**.

   - Caso queira configurar a modelagem de tráfego nas interfaces SD-WAN em um modelo de CPE, acesse a seção **SD-WAN → CPE** do menu, clique no dispositivo CPE e selecione a guia **SD-WAN**. Para editar uma interface SD-WAN herdada do modelo de CPE, marque a caixa de seleção **Substituir** ao lado da interface.

2. Clique na interface SD-WAN que deseja editar, ou ainda, selecione uma interface na tabela e clique no botão **Editar**.

3. Selecione a guia **QoS**.

4. Altere as configurações das filas de tráfego: tags de classes de tráfego, ToS, largura de banda mínima e máxima.

5. Salve as alterações.

Gerenciar classes de tráfego

Sobre classes de tráfego

É possível visualizar a tabela de classes de tráfego num modelo de instância SD-WAN ou no menu de configuração do controlador.

- Para visualizar a tabela de classes de tráfego em um modelo de instância SD-WAN, vá para a seção **SD-WAN→ Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Classes de tráfego**.

- Para visualizar a tabela de classes de tráfego no menu de configurações do controlador, vá para a seção do menu Infraestrutura, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em Configurações de implementação. Depois, vá para a seção QoS.

Por padrão, as seguintes classes de tráfego são criadas:

- **Melhor esforço**
- **Normal para o negócio**
- **Crítico para o negócio**
- **Vídeo**
- **Conferência**
- **Sinalização**
- **Tempo real**
- **Controle de rede**

As informações sobre as classes de tráfego são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da classe de tráfego.
- **Classificar tag** é a tag interna da classe de tráfego.
- **Número da fila** é o número da fila para a qual o tráfego da classe de tráfego vai.
- **KOver** é a taxa de superalocação da largura de banda do tráfego, que define o multiplicador pelo qual a largura de banda dedicada à classe de tráfego pode ser aumentada se a largura de banda total não for totalmente utilizada.
- **Excluir ao computar caminho** indica se a largura de banda disponível para a classe de tráfego é levada em consideração ao calcular a rota:
  - **Sim**.
  - **Não**.

Os seguintes parâmetros são exibidos na parte inferior da tabela:

- **Classe de tráfego padrão** é a classe de tráfego na qual é colocado todo o tráfego não incluído em outras classes.
- **Classe de tráfego de controle** é a classe de tráfego na qual o tráfego de controle usado para gerenciar os componentes da solução é colocado. Recomendamos atribuir a prioridade mais alta ao tráfego de controle para garantir que a rede funcione de forma confiável.
- **Largura máxima de banda reservada (%)** é a porcentagem da taxa máxima de transferência de tráfego que pode estar disponível para a classe de tráfego.

O Kaspersky SD-WAN não é compatível com a criação de classes de tráfego, mas é possível editar as classes de tráfego padrão no modelo de instância SD-WAN ou no menu de configuração do controlador.

Editar uma classe de tráfego

É possível editar uma classe de tráfego num modelo de instância SD-WAN ou no menu de configuração do controlador. Ao editar uma classe de tráfego de um modelo de instância SD-WAN, a classe não é alterada do menu de configuração do controlador de instâncias SD-WAN já implementadas.

> As classes de tráfego padrão são adequadas para a maioria dos cenários de implementação e não é recomendado editá-las.

Para editar uma classe de tráfego:

1. Edite uma classe de tráfego de uma das seguintes formas:

   - Para editar a classe de tráfego num modelo de instância SD-WAN, vá para a seção **SD-WAN → Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Classes de tráfego**.

   - SE você quiser alterar a classe de tráfego no menu de configurações do controlador, vá para a seção do menu Infraestrutura, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em Configurações de implementação. Depois, vá para a seção QoS.

   Uma tabela de classes de tráfego é exibida.

2. Clique em **Editar**.

3. Na coluna **Nome**, insira o nome da classe de tráfego.

4. Na coluna **Número da fila**, selecione o número da fila para onde o tráfego da classe selecionada vai. Quanto maior o valor, maior a prioridade da classe de tráfego. Não é possível especificar a mesma prioridade para várias classes de tráfego.

5. Na coluna **KOver**, selecione a taxa de superalocação da largura de banda do tráfego, que define o multiplicador pelo qual a largura de banda dedicada à classe de tráfego pode ser aumentada se a largura de banda total não for totalmente utilizada.

6. Para ignorar a largura de banda disponível para a classe de tráfego ao criar a rota, marque a caixa de seleção **Excluir ao computar caminho**. Quando essa caixa de seleção está marcada, não é possível selecionar a taxa **KOver** para a classe de tráfego. Por padrão, essa caixa de seleção é marcada ao lado da classe de tráfego **Melhor esforço**.

7. Na lista suspensa **Classe de tráfego padrão**, selecione a classe de tráfego na qual é colocado todo o tráfego não incluído em outras classes. Por padrão, a classe de tráfego **Melhor esforço** é selecionada.

8. Na lista suspensa **Classe de tráfego de controle**, selecione a classe de tráfego na qual deseja que o tráfego de controle seja colocado. Por padrão, a classe de tráfego **Controle de rede** é selecionada.

9. Na lista suspensa **Largura máxima de banda reservada (%)**, selecione a porcentagem da taxa máxima de transferência de tráfego que pode estar disponível para a classe de tráfego. Intervalo de valores: 10 a 90. O valor padrão é **90**.

10. Clique em **Salvar**.

    A classe de tráfego é modificada.

Gerenciar classificadores de tráfego

É possível visualizar a tabela de classificadores de tráfego em um modelo de instância SD-WAN ou no menu de configuração do controlador.

- Para visualizar a tabela de classificadores de tráfego em um modelo de instância SD-WAN, vá para a seção **SD-WAN → Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Classificadores de tráfego**.

- Para visualizar a tabela de classificadores de tráfego no menu de configurações do controlador, vá para a seção do menu Infraestrutura, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em **Configurações de implementação**. Depois, vá para a seção**QoS** e selecione a guia **Classificadores de tráfego**.

Por padrão, é criado o classificador **Untrust-BE-Classifier**, que não confia nos valores DSCP nos campos de cabeçalho do pacote de tráfego e coloca todo o tráfego na classe **Melhor esforço**. As informações sobre as classes de tráfego são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do classificador de tráfego.

- **Tipo** indica se o classificador confia nos valores DSCP definidos nos campos de cabeçalho dos pacotes de tráfego:

  - **Sim**.

  - **Não**.

- **Classe de tráfego** são classes de tráfego nas quais o classificador coloca o tráfego.

- **Campo de pacote** são cabeçalhos de pacotes de tráfego.

- **Tag externa** é o valor DSCP que os cabeçalhos de pacotes de tráfego devem conter para que o classificador coloque o tráfego na classe de tráfego.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um classificador de tráfego

É possível criar um classificador de tráfego num modelo de instância SD-WAN ou no menu de configuração do controlador. Ao criar um classificador de tráfego num modelo de instância SD-WAN, o classificador não é criado no menu de configuração do controlador de instâncias SD-WAN já implementadas.

Para criar um classificador de tráfego:

1. Crie um classificador de tráfego de uma das seguintes formas:

   - Para criar um classificador de tráfego num modelo de instância SD-WAN, vá para a seção **SD-WAN → Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Classificadores de tráfego**.

   - Para criar um classificador de tráfego no menu de configurações do controlador, vá para a seção **Infraestrutura** e clique em **Gerenciamento → Configurações de implementação** ao lado do controlador; então, vá para a seção **QoS** e selecione a guia **Classificadores de tráfego**.

   Uma tabela de classes de tráfego é exibida.

2. Clique em **+Classificador**.

3. Na janela aberta, no campo **Nome**, insira o nome do classificador de tráfego.

4. Na lista suspensa **Tipo**, selecione um dos seguintes valores:

   - **Confiar** significa que o classificador de tráfego confia nos valores DSCP definidos nos campos de cabeçalho dos pacotes de tráfego. Essa é a configuração padrão.

   - **Não confiar** significa que o classificador de tráfego não confia nos valores DSCP configurados nos campos de cabeçalho dos pacotes de tráfego.

5. Caso tenha selecionado **Confiar** na lista **Tipo**, mapeie as classes de tráfego para os valores DSCP nos cabeçalhos dos pacotes de tráfego:

   a. Na coluna **Classe de tráfego**, selecione a classe de tráfego na qual o classificador de tráfego coloca o tráfego.

   b. Na coluna **Tag externa**, clique em **Selecionar** ao lado do campo de cabeçalho do pacote de tráfego.

   c. Marque as caixas de seleção ao lado dos valores DSCP exibidos que devem estar presentes no campo de cabeçalho do pacote de tráfego para que o classificador coloque o tráfego na classe.

   d. Clique em **OK**.

6. Caso tenha selecionado **Não confiar** na lista **Tipo**, selecione a classe de tráfego na qual o classificador coloca todo o tráfego na lista suspensa **Classe de tráfego**.

7. Clique em **Criar**.

   O classificador de tráfego é criado e exibido na tabela.

8. Caso tenha criado um classificador de tráfego no modelo de instância SD-WAN, na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Especifique um classificador de tráfego ao criar ou editar uma regra de qualidade de serviço para fazer com que a regra de qualidade de serviço use esse classificador de tráfego.

Editar um classificador de tráfego

É possível editar um classificador de tráfego num modelo de instância SD-WAN ou no menu de configuração do controlador. Ao editar um classificador de tráfego de um modelo de instância SD-WAN, o classificador não é editado do menu de configuração do controlador de instâncias SD-WAN já implementadas.

Para editar um classificador de tráfego:

1. Edite um classificador de tráfego de uma das seguintes formas:

   - Para editar um classificador de tráfego num modelo de instância SD-WAN, vá para a seção **SD-WAN** → **Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Classificadores de tráfego**.

   - Para editar um classificador de tráfego no menu de configurações do controlador, vá para a seção **Infraestrutura** e clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador; então, vá para a seção **QoS** e selecione a guia **Classificadores de tráfego**.

   Uma tabela de classes de tráfego é exibida.

2. Clique em **Gerenciamento** → **Editar** ao lado do classificador de tráfego que deseja editar.

3. Na janela aberta, se necessário, edite as configurações do classificador de tráfego. Para obter uma descrição das configurações, consulte as instruções para criar um classificador de tráfego.

4. Clique em **Salvar**.

   O classificador de tráfego é modificado e atualizado na tabela.

5. Caso tenha editado um classificador de tráfego no modelo de instância SD-WAN, na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Excluir um classificador de tráfego

É possível excluir um classificador de tráfego num modelo de instância SD-WAN ou no menu de configuração do controlador. Ao excluir um classificador de tráfego de um modelo de instância SD-WAN, o classificador não é excluído do menu de configuração do controlador de instâncias SD-WAN já implementadas.

Os classificadores de tráfego excluídos não podem ser restaurados.

Para excluir um classificador de tráfego:

1. Exclua um classificador de tráfego de uma das seguintes formas:

   - Para excluir um classificador de tráfego num modelo de instância SD-WAN, vá para a seção **SD-WAN → Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Classificadores de tráfego**.

   - Para excluir um classificador de tráfego no menu de configurações do controlador, vá para a seção **Infraestrutura** e clique em **Gerenciamento → Configurações de implementação** ao lado do controlador; então, vá para a seção **QoS** e selecione a guia **Classificadores de tráfego**.

   Uma tabela de classes de tráfego é exibida.

2. Clique em **Gerenciamento → Excluir** ao lado do classificador de tráfego que deseja excluir.

3. Na janela de confirmação, clique em **Excluir**.

   O classificador de tráfego é excluído e não é mais exibido na tabela.

4. Caso tenha excluído um classificador de tráfego no modelo de instância SD-WAN, na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Gerenciar regras de qualidade de serviço

É possível visualizar a tabela de regras de qualidade de serviço num modelo de instância SD-WAN ou no menu de configuração do controlador.

- Para visualizar a tabela de regras de qualidade de serviço em um modelo de instância SD-WAN, vá para a seção **SD-WAN→ Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Regras de QoS**.

- Para visualizar a tabela de regras de qualidade de serviço no menu de configurações do controlador, vá para a seção **Infraestrutura** do menu, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em **Configurações de implementação**. Então, vá para a seção **QoS** e selecione a guia **Regras de QoS**.

Por padrão, é criada a regra de qualidade de serviço **Unlimited-QoS**, que usa o classificador de tráfego padrão, **Untrust-BE-Classifier**, não limita a largura de banda e fornece 100% da largura de banda total à classe de tráfego **Melhor esforço**. As informações sobre regras de qualidade de serviço são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da regra de qualidade de serviço.

- **MBR** é a largura de banda máxima permitida pela regra de qualidade de serviço.

- As seguintes colunas exibem a porcentagem da largura de banda total disponível para as classes de tráfego:

  - **Melhor esforço**

  - **Normal para o negócio**

  - **Crítico para o negócio**

- **Vídeo**
- **Conferência**
- **Sinalização**
- **Tempo real**

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar uma regra de qualidade de serviço

É possível criar uma regra de qualidade de serviço no modelo de instância SD-WAN ou no menu de configuração do controlador. Ao criar uma regra de qualidade de serviço num modelo de instância SD-WAN, a regra não é criada no menu de configuração do controlador de instâncias SD-WAN já implementadas.

Para criar uma regra de qualidade de serviço:

1. Crie uma regra de qualidade de serviço:

   - Para criar uma regra de qualidade de serviço num modelo de instância SD-WAN, vá para a seção **SD-WAN → Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Regras de QoS**.
   - Se você quiser criar uma regra de qualidade de serviço no menu de configurações do controlador, vá para a seção **Infraestrutura** do menu, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em **Configurações de implementação**. Então, vá para a seção **QoS** e selecione a guia **Regras de QoS**.

   A tabela de regras de qualidade de serviço é exibida.

2. Clique em **+ Regra de QoS**.
3. Na janela aberta, no campo **Nome**, insira o nome da regra de qualidade de serviço.
4. Na lista suspensa **Classificador**, selecione o classificador de tráfego criado que deseja usar na regra de qualidade de serviço.
5. Caso deseje que a regra de qualidade de serviço limite a largura de banda para o tráfego processado pelo classificador de tráfego, desmarque a caixa de seleção **Ilimitado**. Esta caixa de seleção é selecionada por padrão.

6. Caso tenha desmarcado a caixa de seleção **Ilimitado**, configure o limite de largura de banda do tráfego:

   a. No campo **MBR**, insira a taxa máxima de bits. O valor padrão é `1`.

   b. Na lista suspensa **Tipo de velocidade**, selecione as unidades de medida para a taxa máxima de bits:

   - **Kbit/s**. Essa é a configuração padrão.
   - **Mbit/s**.
   - **Gbit/s**

   c. Caso tenha selecionado um classificador do tipo **Confiar** na lista suspensa **Classificador**, na coluna **Largura máxima de banda reservada (%)**, especifique a porcentagem da taxa total de bits disponível para as classes de tráfego. A soma total dos valores especificados deve ser igual a 100%.

7. Clique em **Criar**.

   A regra de qualidade de serviço é criada e exibida na tabela.

8. Caso tenha criado uma regra de qualidade de serviço no modelo de instância SD-WAN, clique em **Salvar** na parte superior das configurações para salvar as configurações do modelo de instância SD-WAN.

Especifique uma regra de qualidade de serviço ao criar ou editar um serviço de transporte para fazer com que o serviço de transporte use essa regra.

Editar uma regra de qualidade de serviço

É possível editar uma regra de qualidade de serviço em um modelo de instância SD-WAN ou no menu de configuração do controlador. Ao editar uma regra de qualidade de serviço num modelo de instância SD-WAN, a regra não é editada no menu de configuração do controlador de instâncias SD-WAN já implementadas.

Para editar uma regra de qualidade de serviço:

1. Edite uma regra de qualidade de serviço:

   - Para editar uma regra de qualidade de serviço num modelo de instância SD-WAN, vá para a seção **SD-WAN → Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Regras de QoS**.
   - Se você quiser editar uma regra de qualidade de serviço no menu de configurações do controlador, vá para a seção do menu **Infraestrutura**, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em **Configurações de implementação**. Depois, vá para a seção **QoS** e selecione a guia **Regras de QoS**.

   A tabela de regras de qualidade de serviço é exibida.

2. Clique no nome da regra de qualidade de serviço que deseja editar ou selecione-a na tabela e clique no botão **Editar**.

3. Na janela aberta, se necessário, edite as configurações de qualidade de serviço. Para obter uma descrição das configurações, consulte as instruções para criar uma regra de qualidade de serviço.

4. Clique em **Salvar**.

   A regra de qualidade de serviço é modificada e atualizada na tabela.

5. Caso tenha editado uma regra de qualidade de serviço no modelo de instância SD-WAN, na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Excluir uma regra de qualidade de serviço

É possível excluir uma regra de qualidade de serviço em um modelo de instância SD-WAN ou no menu de configuração do controlador. Ao excluir uma regra de qualidade de serviço num modelo de instância SD-WAN, a regra não é excluída no menu de configuração do controlador de instâncias SD-WAN já implementadas.

As regras de qualidade de serviço excluídas não podem ser restauradas.

Para excluir uma regra de qualidade de serviço:

1. Exclua uma regra de qualidade de serviço:

   - Para excluir uma regra de qualidade de serviço num modelo de instância SD-WAN, vá para a seção **SD-WAN → Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Regras de QoS**.

   - Se você quiser excluir uma regra de qualidade de serviço no menu de configurações do controlador, vá para a seção do menu **Infraestrutura**, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em **Configurações de implementação**. Depois, vá para a seção **QoS** e selecione a guia **Regras de QoS**.

   A tabela de regras de qualidade de serviço é exibida.

2. Selecione a regra de qualidade de serviço que deseja excluir e clique no botão **Excluir**.

3. Na janela de confirmação, clique em **Excluir**.

   A regra de qualidade de serviço é excluída e não é mais exibida na tabela.

4. Caso tenha excluído uma regra de qualidade de serviço no modelo de instância SD-WAN, na parte inferior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Gerenciar restrições de Manual-TE

Para visualizar a tabela de restrições de Manual-TE, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento → Configurações de implementação** ao lado do controlador e vá para a seção **Restrições**. As informações sobre as restrições de Manual-TE são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da restrição de Manual-TE.
- **Segmento** é o segmento dos caminhos de Manual-TE adicionados à restrição de Manual-TE.
- **Caminhos** são os caminhos de Manual-TE adicionados à restrição de Manual-TE.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar uma restrição de Manual-TE

Para criar uma restrição de Manual-TE:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Restrições**.

   A guia **TE manual** com a tabela de restrições de Manual-TE é selecionada por padrão.

4. Na parte superior da página, clique em **+ Adicionar**.

5. Na janela aberta, no campo **Nome**, insira o nome da restrição de Manual-TE.

6. Marque a caixa de seleção **Usar caminho de TE manual** ao lado dos caminhos de Manual-TE criados que deseja adicionar à restrição de Manual-TE. Essas caixas de seleção são desmarcadas por padrão.

7. Para permitir o uso de um caminho de Auto-SPF quando os caminhos de Manual-TE especificados não estiverem disponíveis, marque a caixa de seleção **Ignorar se nenhum caminho restrito for encontrado** ao lado dos caminhos de Manual-TE. Só é possível marcar a caixa de seleção ao lado de um caminho de Manual-TE com a caixa de seleção **Usar caminho de TE manual** marcada. Essas caixas de seleção são desmarcadas por padrão.

8. Clique em **Criar**.

A restrição de Manual-TE é criada e exibida na tabela.

É possível especificar uma restrição de Manual-TE ao criar ou editar um serviço de transporte para que ele use essa restrição.

Editar uma restrição de Manual-TE

Para editar uma restrição de Manual-TE:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Restrições**.

   A guia **TE manual** com a tabela de restrições de Manual-TE é selecionada por padrão.

4. Clique no nome da regra Manual-TE que deseja editar ou selecione-a na tabela e clique no botão **Editar**.

5. Na janela aberta, se necessário, edite as configurações da restrição de Manual-TE. Para obter uma descrição das configurações, consulte as instruções para criar uma restrição de Manual-TE.

6. Clique em **Salvar**.

A restrição de Manual-TE é modificada e atualizada na tabela.

Excluir uma restrição de Manual-TE

As restrições de Manual-TE excluídas não podem ser restauradas.

Para excluir uma restrição de Manual-TE:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Restrições**.

   A guia **TE manual** com a tabela de restrições de Manual-TE é selecionada por padrão.

4. Na tabela, selecione a restrição Manual-TE que deseja excluir e clique no botão **Excluir**.

5. Na janela de confirmação, clique em **Excluir**.

A restrição de Manual-TE é excluída e não é mais exibida na tabela.

Gerenciar restrições de limite

Para visualizar a tabela de restrições de limite no menu de configurações do controlador, vá para a seção de menu **Infraestrutura**, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em **Configurações de implementação**. Depois, vá para a seção **Restrições** e selecione a guia **Limites**. As informações sobre as restrições de limite são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da restrição de limite.
- **Último recurso** indica se a restrição de limite exclui um link do cálculo do caminho Auto-TE caso a caixa de seleção **Último recurso** esteja marcada nas configurações de monitoramento de link:
  - Y
  - N
- **Nível do erro** indica se a restrição de limite exclui um link do cálculo do caminho Auto-TE se o limite de erros por segundo for atingido no link:
  - Y
  - N
- **Utilização** indica se a restrição de limite exclui um link do cálculo do caminho Auto-TE se o limite de utilização for atingido no link, na forma de uma porcentagem da largura de banda da interface de serviço de origem:
  - Y
  - N
- **Latência** indica se a restrição de limite exclui um link do cálculo do caminho Auto-TE se o limite de atraso (em milissegundos) for atingido no tráfego que passa pelo link:
  - Y
  - N
- **Jitter** indica se a restrição de limite exclui um link do cálculo do caminho Auto-TE se o limite de jitter (em milissegundos) for atingido no tráfego que passa pelo link:
  - Y
  - N
- **Perda de pacotes** indica se a restrição de limite exclui um link do cálculo do caminho Auto-TE se o limite de perda de pacotes (como um valor percentual) for atingido no link:
  - Y
  - N

É possível especificar limites de monitoramento ao configurar o monitoramento de links.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar uma restrição de limite

Para criar uma restrição de limite:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Restrições**.

   A guia **TE manual** com a tabela de restrições de Manual-TE é selecionada por padrão.

4. Selecione a guia **Limites**.

   É exibida uma tabela de restrições de limite.

5. Na parte superior da página, clique em **+ Restrição de limite**.

6. Na janela aberta, no campo **Nome**, insira o nome da restrição de limite.

7. Marque a caixa de seleção **Não usar links com limite alcançado** ao lado de indicadores de monitoramento de link para que a restrição de limite exclua links que tenham atingido o limite desses indicadores de monitoramento do cálculo do caminho de Auto-TE. Esta caixa de seleção está desmarcada por padrão.

8. Caso não queira que a restrição de limite exclua links com limites atingidos do cálculo do caminho de Auto-TE quando não existirem links alternativos, marque a caixa de seleção **Ignorar se nenhum caminho restrito for encontrado** ao lado dos valores de monitoramento. Esta caixa de seleção está desmarcada por padrão. Só é possível marcar a caixa de seleção ao lado de valores de monitoramento com a caixa de seleção **Não usar links com limite alcançado** marcada.

   Por exemplo, caso tenha marcado a caixa de seleção **Não usar links com limite alcançado** ao lado do valor de monitoramento **Nível do erro**, a restrição de limite exclui do cálculo do caminho de Auto-TE um link em que o limite de erros por segundo é alcançado. Caso também tenha marcado a caixa de seleção **Ignorar se nenhum caminho restrito for encontrado** e todos os links atinjam o limite de erros por segundo, a restrição de limite não excluirá o link do cálculo do caminho de Auto-TE.

9. Clique em **Criar**.

A restrição de limite é criada e exibida na tabela.

É possível especificar uma restrição de limite ao criar ou editar um serviço de transporte para que o serviço de transporte use essa restrição.

Editar uma restrição de limite

Para editar uma restrição de limite:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Restrições**.

   A guia **TE manual** com a tabela de restrições de Manual-TE é selecionada por padrão.

4. Selecione a guia **Limites**.

   É exibida uma tabela de restrições de limite.

5. Clique no nome da restrição de limite que deseja editar ou selecione-a na tabela e clique no botão **Editar**.

6. Na janela aberta, se necessário, edite as configurações da restrição de limite. Para obter uma descrição das configurações, consulte as instruções para criar uma restrição de limite.

7. Clique em **Salvar**.

A restrição de limite é modificada e atualizada na tabela.

Excluir uma restrição de limite

As restrições de limite excluídas não podem ser restauradas.

Para excluir uma restrição de limite:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Restrições**.

   A guia **TE manual** com a tabela de restrições de Manual-TE é selecionada por padrão.

4. Selecione a guia **Limites**.

   É exibida uma tabela de restrições de limite.

5. Na tabela, selecione a restrição de limite que deseja excluir e clique no botão **Excluir**.

6. Na janela de confirmação, clique em **Excluir**.

A restrição de limite é excluída e não é mais exibida na tabela.

Gerenciar regras de classificação de tráfego

Para visualizar a tabela de regras de classificação de tráfego, no menu de configurações do controlador, vá para a seção do menu **Infraestrutura**, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em **Configurações de implementação**. Depois, vá para a seção **Filtros de tráfego**.

As informações sobre regras de classificação de tráfego são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome da regra de classificação de tráfego.
- **Campos L2** são campos L2 cujos valores a regra de classificação de tráfego usa para identificar o tráfego no fluxo de dados geral.
- **Campos L3** são campos L3 cujos valores a regra de classificação de tráfego usa para identificar o tráfego no fluxo de dados geral.
- **Campos L4** são campos L4 cujos valores a regra de classificação de tráfego usa para identificar o tráfego no fluxo de dados geral.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar uma regra de classificação de tráfego

Para criar uma regra de classificação de tráfego:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Filtros de tráfego**.

   Por padrão, é selecionada a guia **Regras**, que exibe a tabela de regras de classificação de tráfego.

4. Na parte superior da página, clique em **+ Regra de qualificação**.

5. Na janela aberta, no campo **Nome**, insira o nome da regra de classificação de tráfego.

6. Na guia **Campos L2**, marque as caixas de seleção ao lado dos campos L2 cujos valores a regra de classificação de tráfego usa para identificar o tráfego no fluxo de dados geral. Se a caixa de seleção estiver marcada, insira ou selecione o valor do campo. É possível usar os valores dos seguintes campos para identificar o tráfego no fluxo de dados geral:

   - **ID da VLAN externa**. Intervalo de valores: 1 a 2094.
   - **PCP da VLAN externa**. Intervalo de valores: 0 a 7.
   - **MAC de origem**.
   - **Máscara MAC de origem**.
   - **MAC de destino**.
   - **Máscara MAC de destino**.
   - **Ethertype**:
     - **0x0800**. Essa é a configuração padrão.
     - **0x86dd**
     - **0x0806**

7. Na guia **Campos L3**, marque as caixas de seleção ao lado dos campos L3 cujos valores a regra de classificação de tráfego usa para identificar o tráfego no fluxo de dados geral. Se a caixa de seleção estiver marcada, insira ou selecione o valor do campo. É possível usar os valores dos seguintes campos para identificar o tráfego no fluxo de dados geral.

   - **Protocolo**:
     - **IPv4**
     - **IPv6**
   - **IP de origem**.
   - **Comprimento do prefixo de IP de origem**. Intervalo de valores para o endereço IPv4: 0 a 32; para o endereço IPv6: 0 a 128
   - **IP de destino**.
   - **Comprimento do prefixo de IP de destino**. Intervalo de valores para o endereço IPv4: 0 a 32; para o endereço IPv6: 0 a 128
   - **DSCP**
   - **TOS**

8. Na guia **Campos L4**, marque as caixas de seleção ao lado dos campos L4 cujos valores a regra de classificação de tráfego usa para identificar o tráfego no fluxo de dados geral. Se a caixa de seleção estiver marcada, insira ou selecione o valor do campo. É possível usar os valores dos seguintes campos para identificar o tráfego no fluxo de dados geral:

   - **Protocolo IP**
   - **Lista de portas de origem**
   - **Lista de portas de destino**
   - **Número de tipo ICMP**

9. Na guia **DPI**, marque a caixa de seleção **Aplicativo** e selecione o aplicativo cujo tráfego a regra de classificação de tráfego identifica no fluxo de dados geral.

10. Clique em **Criar**.

    A regra de classificação de tráfego é criada e exibida na tabela.

É possível especificar uma regra de classificação de tráfego ao criar ou editar um filtro de tráfego para que ele use essa regra.

Exemplo de uma regra de classificação de tráfego criada:
É possível criar uma regra de classificação de tráfego com os seguintes parâmetros:

- Na guia **Campos L2**, no campo **ID da VLAN externa**, insira `1`.
- Na guia **Campos L2**, no campo **PCP da VLAN externa**, insira `3`.
- Na guia **Campos L3**, na lista suspensa **Protocolo**, selecione **IPv4**.
- Na guia **Campos L3**, no campo **IP de origem**, insira o endereço IP `192.168.2.0/24`.

A regra de classificação de tráfego identifica tráfego com as seguintes propriedades no fluxo de dados geral:

- Tag de VLAN externa — 1
- Tag de PCP externa — 3
- Protocolo — IPv4
- Endereço IP de origem — 192.168.2.0/24

A regra de classificação de tráfego não identifica tráfego que não tenha pelo menos uma dessas propriedades no fluxo de dados geral.

Editar uma regra de classificação de tráfego

Para editar uma regra de classificação de tráfego:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Filtros de tráfego**.

   Por padrão, é selecionada a guia **Regras**, que exibe a tabela de regras de classificação de tráfego.

4. Clique no nome da regra de classificação de tráfego que deseja editar ou selecione-a na tabela e clique no botão **Editar**.

5. Na janela aberta, se necessário, edite as configurações da regra de classificação de tráfego. Para obter uma descrição das configurações, consulte as instruções para criar uma regra de classificação de tráfego.

6. Clique em **Salvar**.

A regra de classificação de tráfego é modificada e atualizada na tabela.

Excluir uma regra de classificação de tráfego

As regras de classificação de tráfego excluídas não podem ser restauradas.

Para excluir uma regra de classificação de tráfego:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Filtros de tráfego**.

   Por padrão, é selecionada a guia **Regras**, que exibe a tabela de regras de classificação de tráfego.

4. Na tabela, selecione a regra de classificação de tráfego que deseja excluir e clique no botão **Excluir**.

5. Na janela de confirmação, clique em **Excluir**.

A regra de classificação de tráfego é excluída e não é mais exibida na tabela.

Gerenciar filtros de tráfego

Para visualizar a tabela de filtros de tráfego no menu de configurações do controlador, vá para a seção do menu **Infraestrutura**, abra as configurações de implementação do controlador clicando no nome do controlador ou selecionando o controlador na tabela e clicando em **Configurações de implementação**. Depois, vá para a seção **Filtros de tráfego** e selecione a guia **Filtros**. As informações sobre os filtros de tráfego são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do filtro de tráfego.
- **Regras adicionadas** são as regras de classificação de tráfego adicionadas ao filtro de tráfego.

- **Ação** é a ação que o filtro de tráfego aplica ao tráfego:
  - **Permitir** — Permitir o encaminhamento adicional do tráfego.
  - **Negar** — Bloquear o encaminhamento adicional do tráfego.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um filtro de tráfego

Para criar um filtro de tráfego:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Filtros de tráfego**.

   Por padrão, é selecionada a guia **Regras**, que exibe a tabela de regras de classificação de tráfego.

4. Selecione a guia **Filtros**.

   Uma tabela de filtros de tráfego é exibida.

5. Na parte superior da página, clique em **+ Filtro de tráfego**.

6. Na janela aberta, no campo **Nome**, insira o nome do filtro de tráfego.

7. Adicione a regra de classificação de tráfego criada ao filtro de tráfego:

   a. No campo **Sequência**, insira o número sequencial da regra de classificação de tráfego. A primeira regra de classificação de tráfego aplicada pelo filtro é a regra com o menor número sequencial. Intervalo de valores: 1 a 998. O valor padrão é `10`.

      Não é possível especificar o mesmo número sequencial para mais de uma regra de classificação de tráfego.

   b. Na lista suspensa **Regra de qualificação**, selecione a regra de classificação de tráfego que deseja adicionar ao filtro de tráfego.

   c. Na lista suspensa **Ação**, selecione a ação que o filtro de tráfego aplica ao tráfego:

      - **Permitir** — Permitir o encaminhamento adicional do tráfego. Essa é a configuração padrão.
      - **Negar** — Bloquear o encaminhamento adicional do tráfego.

   d. Clique em **Adicionar**.

A regra de classificação de tráfego é adicionada. É possível adicionar várias regras de classificação de tráfego ou excluir regras de classificação de tráfego. Para excluir uma regra de classificação de tráfego, clique em **Excluir** ao lado dele.

8. Na lista suspensa **Ação padrão**, selecione a ação que o filtro de tráfego aplica a todo o restante do tráfego:

   - **Permitir** — Permitir o encaminhamento adicional do tráfego. Essa é a configuração padrão.
   - **Negar** — Bloquear o encaminhamento adicional do tráfego.

9. Clique em **Criar**.

O filtro de tráfego é criado e exibido na tabela.

É possível especificar um filtro de tráfego ao criar ou editar um serviço de transporte ou uma interface ACL para que o serviço de transporte ou a interface ACL usem esse filtro de tráfego.

Editar um filtro de tráfego

Para editar um filtro de tráfego:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Filtros de tráfego**.

   Por padrão, é selecionada a guia **Regras**, que exibe a tabela de regras de classificação de tráfego.

4. Selecione a guia **Filtros**.

   Uma tabela de filtros de tráfego é exibida.

5. Clique no nome do filtro de tráfego que deseja editar ou selecione-o na tabela e clique no botão **Editar**.

6. Na janela aberta, se necessário, edite as configurações do filtro de tráfego. Para obter uma descrição das configurações, consulte as instruções para criar um filtro de tráfego.

7. Clique em **Salvar**.

O filtro de tráfego é modificado e atualizado na tabela.

Excluir um filtro de tráfego

Os filtros de tráfego excluídos não podem ser restaurados.

Para excluir um filtro de tráfego:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Filtros de tráfego**.

   Por padrão, é selecionada a guia **Regras**, que exibe a tabela de regras de classificação de tráfego.

4. Selecione a guia **Filtros**.

   Uma tabela de filtros de tráfego é exibida.

5. Na tabela, selecione o filtro de tráfego que deseja excluir e clique no botão **Excluir**.

6. Na janela de confirmação, clique em **Excluir**.

O filtro de tráfego é excluído e não é mais exibido na tabela.

Transmissão de tráfego entre dispositivos CPE e dispositivos cliente usando serviços de transporte

Sobre serviços de transporte

Use *serviços de transporte* para transmitir tráfego entre dispositivos CPE e dispositivos cliente conectados a eles. Os serviços de transporte são criados com base em segmentos e consistem em interfaces de serviço. O Kaspersky SD-WAN oferece suporte à criação dos seguintes serviços de transporte:

- L2:
  - Ponto a ponto (E-line na classificação MEF, doravante também referido como serviço P2P) é um serviço de transporte estático em que o tráfego é transmitido entre duas interfaces de serviço.
  - Ponto-a-Multiponto (E-tree na classificação MEF, doravante também referido como serviço P2M) é um serviço de transporte em que o tráfego é transmitido entre múltiplas interfaces de serviço de acordo com uma topologia em árvore. Para cada interface de serviço adicionada ao serviço P2M, é necessário atribuir uma das seguintes funções:
    - **Raiz** significa que a interface de serviço pode enviar tráfego para interfaces de serviço com qualquer função.
    - **Folha** significa que a interface de serviço pode enviar tráfego apenas para interfaces de serviço com a função **Raiz**.
  - Multiponto-a-Multiponto (E-LAN na classificação MEF, doravante também referido como serviço M2M) é um serviço de transporte em que o tráfego é transmitido entre múltiplas interfaces de serviço sem uma hierarquia.

  O serviço P2P é um serviço de transporte estático e não usa o mecanismo de aprendizado MAC para preencher a tabela MAC no Controlador. Os endereços MAC são adicionados automaticamente à tabela MAC no controlador quando um serviço P2P é criado ou modificado. O mecanismo de aprendizado de endereço MAC é usado para serviços P2M e M2M.
- O multicast IP (doravante também referido como serviço multicast IP) é um serviço de transporte em que uma árvore multicast é criada para a distribuição de tráfego entre várias interfaces de serviço.
- VPN L3 (doravante também referido como serviço de VPN L3) é um serviço de transporte em que o tráfego é roteado entre múltiplas interfaces L3, que são mapeadas para interfaces de serviço ou serviços M2M.

Ao criar ou editar serviços de transporte, é possível adicionar interfaces de serviço de backup. Uma interface de serviço de backup permite continuar a transferência de dados em caso de falha da interface de serviço principal. As interfaces de serviço principal e de backup podem ser criadas no mesmo dispositivo CPE ou em dispositivos CPE diferentes.

O tráfego pode ser espelhado ou encaminhado entre interfaces de serviço de dispositivos CPE. Nesse caso, as interfaces de serviço podem ser adicionadas ao serviço de transporte.

Gerenciar serviços de transporte em um modelo de instância SD-WAN ou de CPE

É possível criar serviços P2M e M2M, bem como serviços de VPN L3, em um modelo de instância SD-WAN e usá-lo ao implementar uma instância SD-WAN. Os serviços de transporte criados no modelo de instância SD-WAN são criados automaticamente para a instância SD-WAN implementada. Dessa forma, é possível criar serviços de transporte antes de implementar a instância SD-WAN.

Os serviços de transporte criados para uma instância de SD-WAN implementada podem ser adicionados a um modelo de CPE e, em seguida, é possível especificar o modelo ao adicionar ou registrar dispositivos CPE manualmente. Isso automaticamente cria interfaces de serviço que são mapeadas para portas OpenFlow, que, por sua vez, são mapeadas para interfaces SD-WAN do tipo LAN de dispositivos CPE. As interfaces de serviço criadas automaticamente são adicionadas aos serviços de transporte adicionados ao modelo de CPE. Dessa forma, não é necessário estabelecer a conexão manual de cada dispositivo CPE aos serviços de transporte.

Serviço de transporte de gerenciamento

Quando um dispositivo CPE é registrado, ele se conecta automaticamente a um serviço de transporte de gerenciamento. O serviço de transporte de gerenciamento transmite o tráfego do console SSH, executa scripts e envia comandos de API para gerenciar o VIM implementado em um dispositivo uCPE.

Por padrão, um serviço de transporte de gerenciamento P2M é criado em cada modelo de instância SD-WAN. Ao criar ou editar um serviço P2M ou M2M no modelo de instância SD-WAN, é possível tornar esse serviço P2M ou M2M o serviço de gerenciamento.

Se necessário, o tráfego de monitoramento do Zabbix, assim como o tráfego do protocolo syslog e NetFlow, podem ser transmitidos através do serviço de transporte de gerenciamento. O tráfego de monitoramento do Zabbix é criptografado por padrão, mas para criptografar o tráfego syslog e NetFlow, esse tráfego deve ser transmitido através do serviço de transporte de gerenciamento. A transmissão do tráfego syslog e NetFlow através do serviço de transporte de gerenciamento é regida pelas configurações da tabela de roteamento e encaminhamento do dispositivo CPE.

Duplicação de pacotes de tráfego

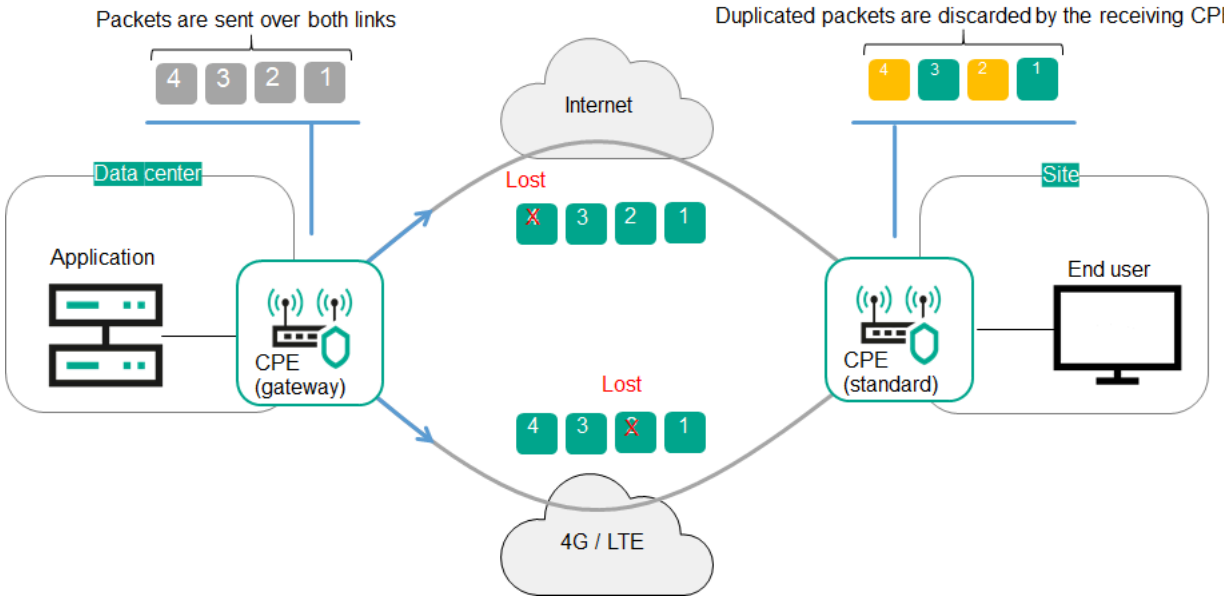
É possível ativar a duplicação de pacotes de tráfego para evitar perdas ao transmitir pacotes de tráfego através dos seguintes serviços de transporte:

- Serviços P2P
- Serviços P2M
- Serviços M2M
- Serviços de L3 VPN
- Serviços TAP

Se a duplicação de pacotes de tráfego estiver ativada em um serviço de transporte, o dispositivo CPE de origem duplica os pacotes de tráfego e os envia por meio de todas as conexões. O dispositivo CPE de destino recebe os pacotes de tráfego e descarta os pacotes de tráfego supérfluos. Se um pacote de tráfego enviado por meio de uma conexão for perdido, o dispositivo CPE de destino recebe esse pacote de tráfego por meio de outra conexão. A duplicação de pacotes de tráfego pode ser usada para aplicativos com alta demanda, como caixas eletrônicos e terminais de PDV.

Para ativar a duplicação de pacotes de tráfego, selecione **Difusão** na lista suspensa **Modo de balanceamento** ao criar ou editar um serviço de transporte.

Por exemplo, a figura abaixo mostra um dispositivo CPE com a função de gateway em um data center. Esse dispositivo CPE usa duas conexões para enviar pacotes de tráfego para um dispositivo CPE padrão em um local remoto. O dispositivo CPE padrão no local remoto então retransmite os pacotes de tráfego aos usuários finais. Ambos os dispositivos CPE são adicionados a um serviço de transporte com a duplicação de pacotes de tráfego ativada, o que significa que os pacotes de tráfego são duplicados e transmitidos simultaneamente por meio de duas conexões.



Duplicação de pacotes de tráfego entre dispositivos CPE

Cenário: direcionar o tráfego do aplicativo para um serviço de transporte

O cenário para direcionar o tráfego do aplicativo para um serviço de transporte envolve as seguintes etapas:

1. **Criar um serviço de transporte**

   Crie o serviço de transporte para o qual deseja direcionar o tráfego do aplicativo. É possível usar as seguintes instruções para concluir esta etapa:

   - Criar um serviço P2P
   - Criar um serviço P2M
   - Criar um serviço M2M
   - Criar um serviço multicast IP
   - Criar um serviço de VPN L3

2. **Criar uma regra de classificação de tráfego**

   Crie uma regra de classificação de tráfego para identificar o tráfego do aplicativo no fluxo de dados geral. Ao criar uma regra de classificação de tráfego, selecione o protocolo L3 na guia **Campos L3** e selecione o aplicativo cujo tráfego deseja direcionar para o serviço de transporte na guia **DPI**.

   Para direcionar o tráfego de vários aplicativos para um serviço de transporte, crie uma regra de classificação de tráfego para cada aplicativo.

3. **Criar um filtro de tráfego**

   Crie um filtro de tráfego para determinar se o roteamento do tráfego do aplicativo é permitido. Ao criar um filtro de tráfego, adicione ao filtro as regras de classificação de tráfego criadas para o tráfego do aplicativo.

4. **Criar uma interface ACL**

   Crie uma interface ACL para aplicar o filtro de tráfego ao tráfego transmitido por meio dessa interface ACL. Ao criar uma interface ACL, selecione um filtro de tráfego criado para o tráfego do aplicativo.

5. **Adicionar a interface ACL ao serviço de transporte**

   Edite o serviço de transporte para adicionar a interface ACL criada para o tráfego do aplicativo. É possível usar as seguintes instruções para concluir esta etapa:

   - Editar um serviço P2P
   - Editar um serviço P2M
   - Editar um serviço M2M
   - Editar um serviço multicast IP
   - Editar um serviço de VPN L3

O tráfego do aplicativo é direcionado para o serviço de transporte.

Cenário: estabelecer conectividade L2 entre dispositivos CPE

É possível estabelecer uma conexão L2 entre dispositivos CPE para as seguintes finalidades:

- Criar um domínio L2 que inclui diversos locais remotos.
- Transmitir tráfego L2 para links keepalive entre dispositivos CPE instalados em locais remotos diferentes.
- Implementar cenários de espelhamento de tráfego personalizados.

O cenário para estabelecer uma conexão L2 entre dispositivos CPE envolve as seguintes etapas:

1 **Criar portas OpenFlow em switches virtuais de dispositivos CPE**

1. Ao criar ou editar uma interface de rede sem um endereço IP em dispositivos CPE entre os quais se deseja estabelecer a conexão L2, marque a caixa de seleção **Modo L2**. Quando a caixa de seleção é marcada, uma porta OpenFlow mapeada para a interface de rede é criada automaticamente no switch virtual do dispositivo CPE. Esta caixa de seleção está desmarcada por padrão. Não é possível marcar essa caixa de seleção nos seguintes casos:

   - As seguintes caixas de seleção foram marcadas ao criar uma interface de rede:
     - **Ponte**
     - **NetFlow**
     - **Forçar endereço IP, rota e gateway**
   - A interface de rede é usada em uma rota estática.
   - A interface de rede é usada pelo BGP.
   - A interface de rede é usada pelo protocolo OSPF.
   - A interface de rede é usada pelo protocolo VRRP.
   - A interface de rede é usada para transmitir o tráfego multicast.
   - A interface de rede é usada por uma tabela de roteamento e encaminhamento virtual (VRF).
   - A interface de rede é usada para diagnóstico do dispositivo CPE usando os utilitários ping, traceroute, tcpdump e/ou sweep.

   O número da porta OpenFlow criada automaticamente no switch virtual do dispositivo CPE é exibido no campo **Porta OpenFlow**. É possível alterar o número da porta OpenFlow. Intervalo de valores: 11 a 20.

1 **Criar interfaces de serviço mapeadas para portas OpenFlow**

Crie interfaces de serviço mapeadas para as portas OpenFlow criadas automaticamente na etapa anterior deste cenário. É necessário selecionar a porta OpenFlow para a qual a interface de serviço está mapeada na lista suspensa **Porta**.

2 **Adicionar interfaces de serviço ao serviço de transporte**

Adicione as interfaces de serviço criadas na etapa anterior deste cenário ao serviço de transporte que deseja usar para estabelecer a conexão L2 entre dispositivos CPE. É possível usar as seguintes instruções para concluir esta etapa:

- Criar um serviço P2P e Editar um serviço P2P.
- Criar um serviço P2M e Editar um serviço P2M.
- Criar um serviço M2M e Editar um serviço M2M.
- Criar um serviço de VPN L3 e Editar um serviço de VPN L3.

- Criar um serviço multicast IP e Editar um serviço multicast IP.
- Criar um serviço TAP e Editar um serviço TAP.

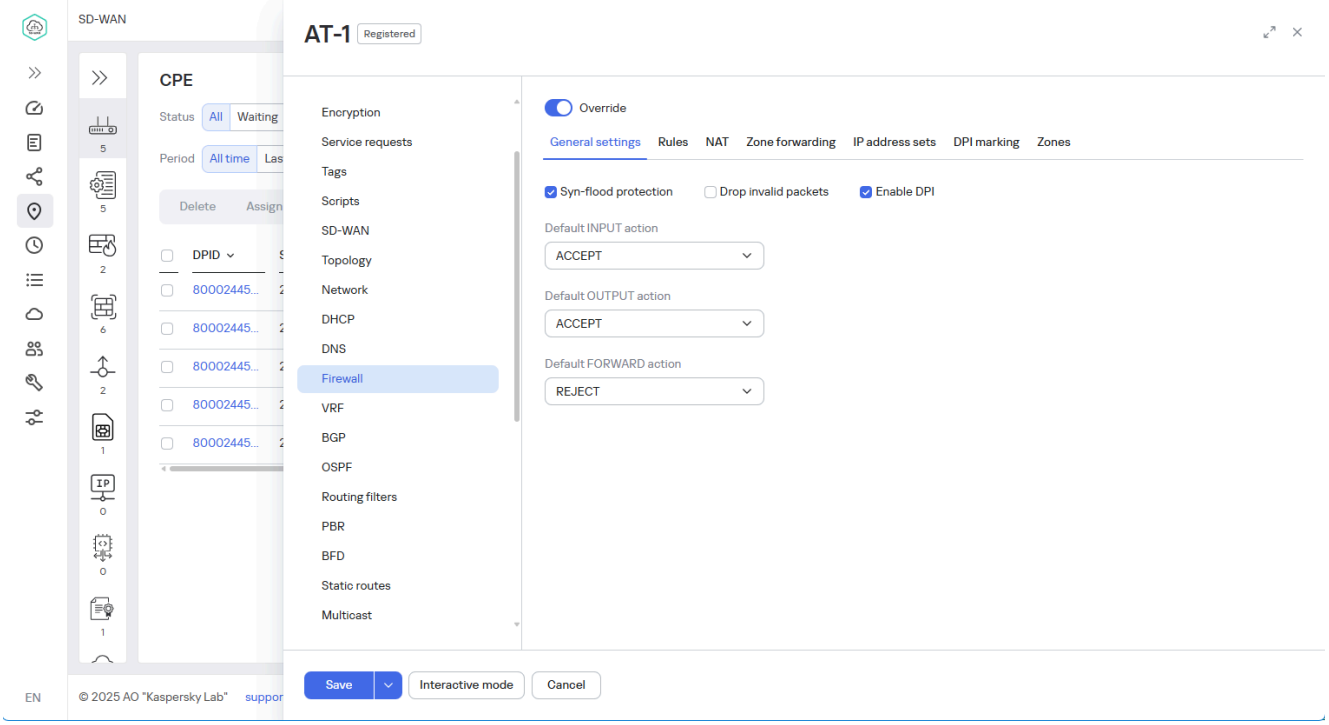
A conexão L2 entre dispositivos CPE é estabelecida.

Cenário: gerenciar o tráfego do aplicativo de acordo com um SLA

O cenário para gerenciar o tráfego do aplicativo de acordo com um SLA envolve as seguintes etapas:

1. **Ativar a DPI (Inspeção profunda de pacotes) globalmente nas configurações do firewall**

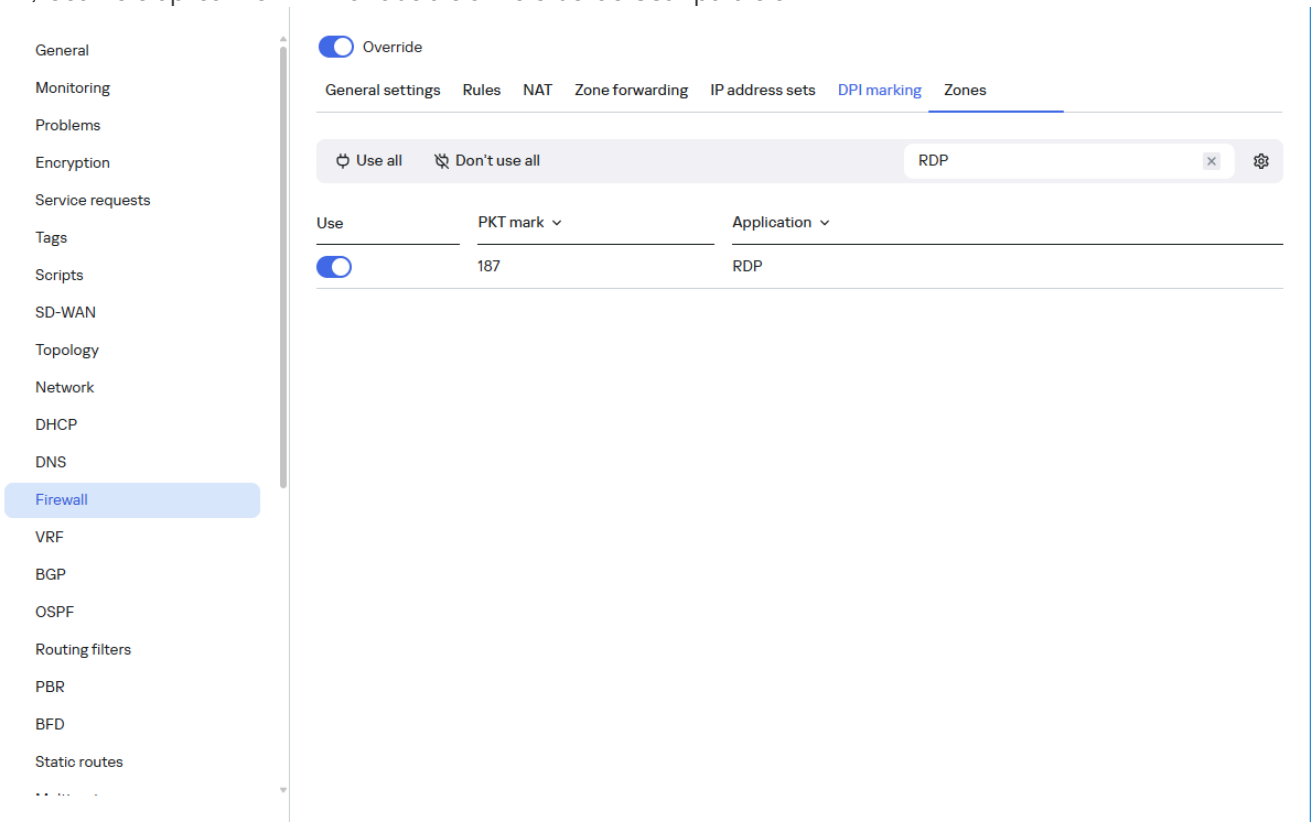
   Certifique-se de que na área de **principais configurações do firewall** do dispositivo CPE ou do modelo de firewall, a caixa de seleção Ativar DPI esteja marcada:



Janela de configurações do CPE. Ativar a funcionalidade DPI.

2. **Ativar o reconhecimento de aplicativo usando DPI para RDP**

Na área de configurações do firewall do dispositivo CPE ou modelo de firewall, selecione a guia **Marcação de DPI**, localize o aplicativo **RDP** na tabela e ative o botão **Usar** para ele:

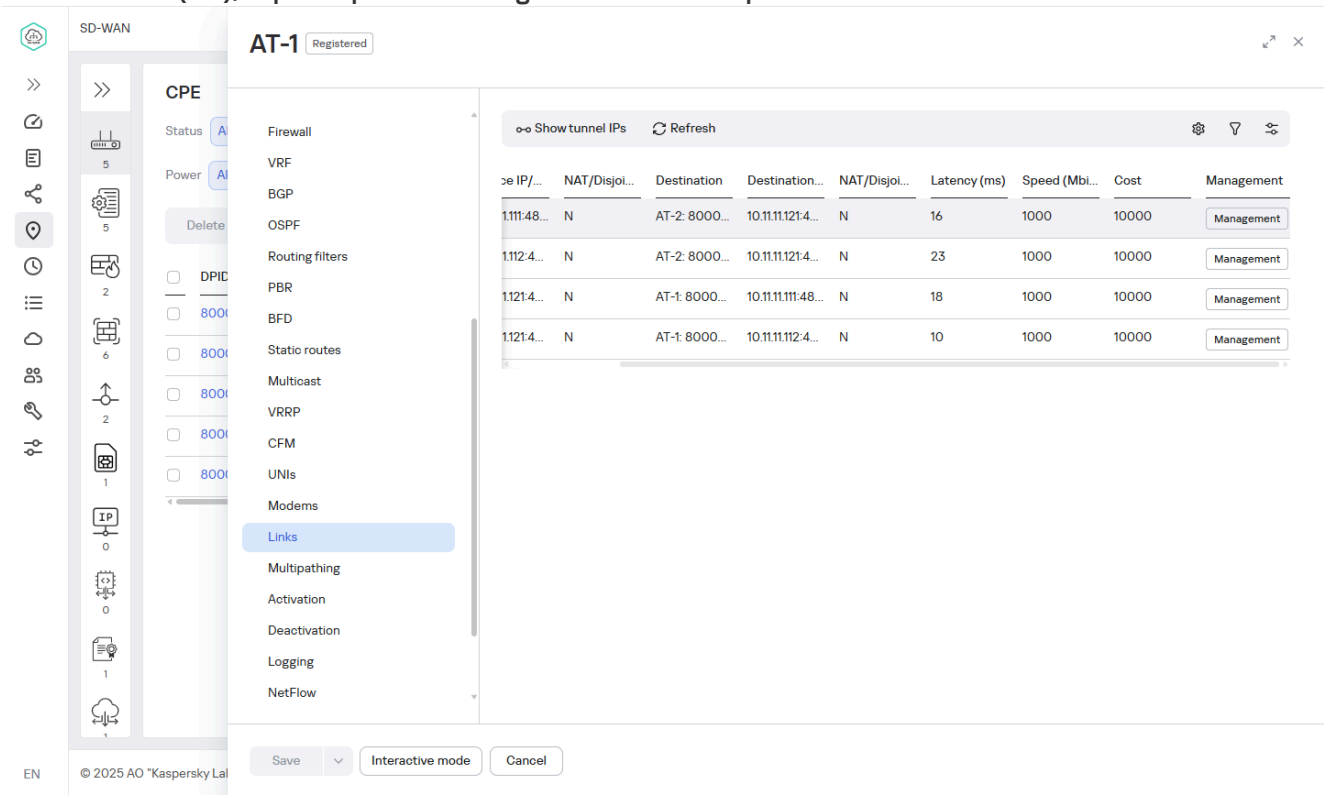


Ativar o DPI para o reconhecimento de RDP

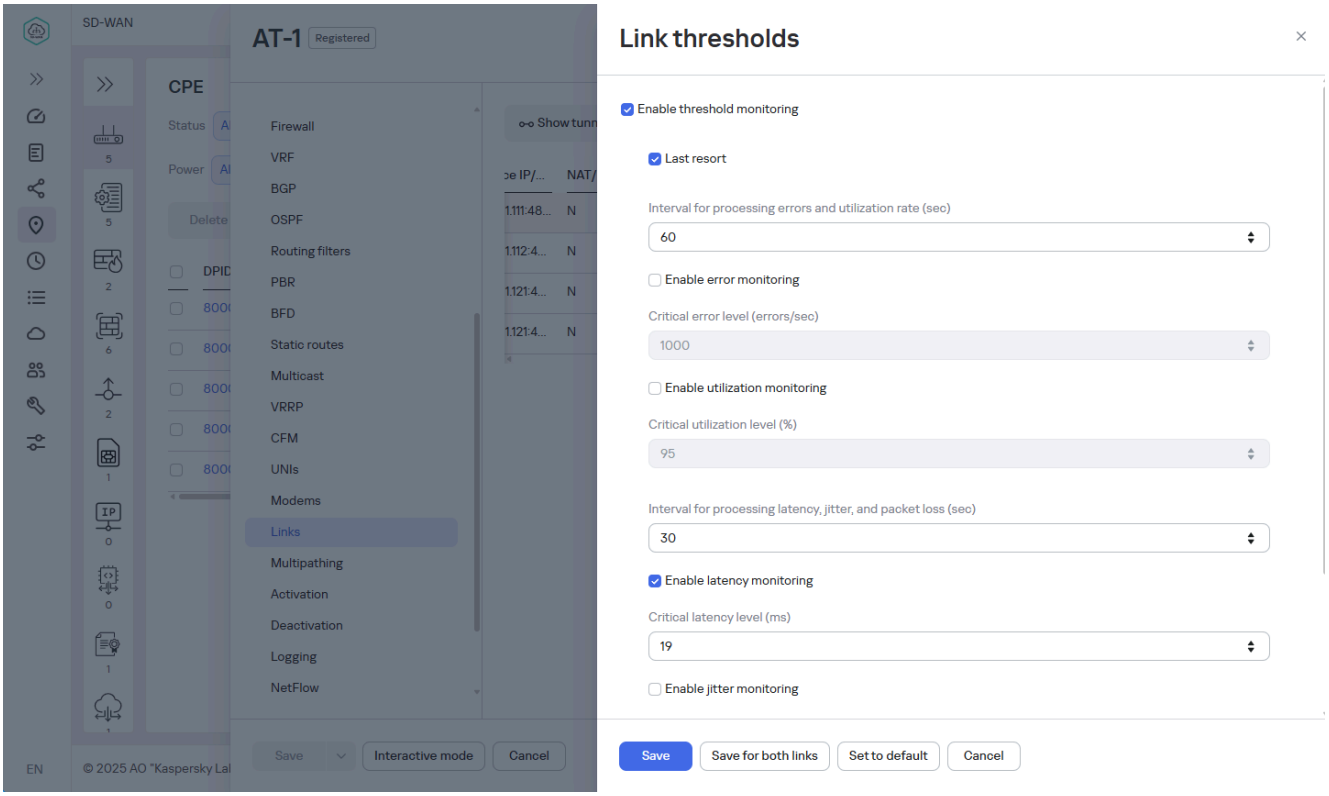
Para obter mais informações sobre como configurar a DPI, consulte Configurar a marcação de DPI.

3. Ativar o monitoramento de tráfego em links CPE

Siga as instruções de Monitoramento de link para ativar o monitoramento de limite no link relevante do dispositivo CPE, marque a caixa de seleção Último recurso e, para a configuração Nível crítico de latência (ms), especifique um valor ligeiramente maior que a latência no link selecionado:



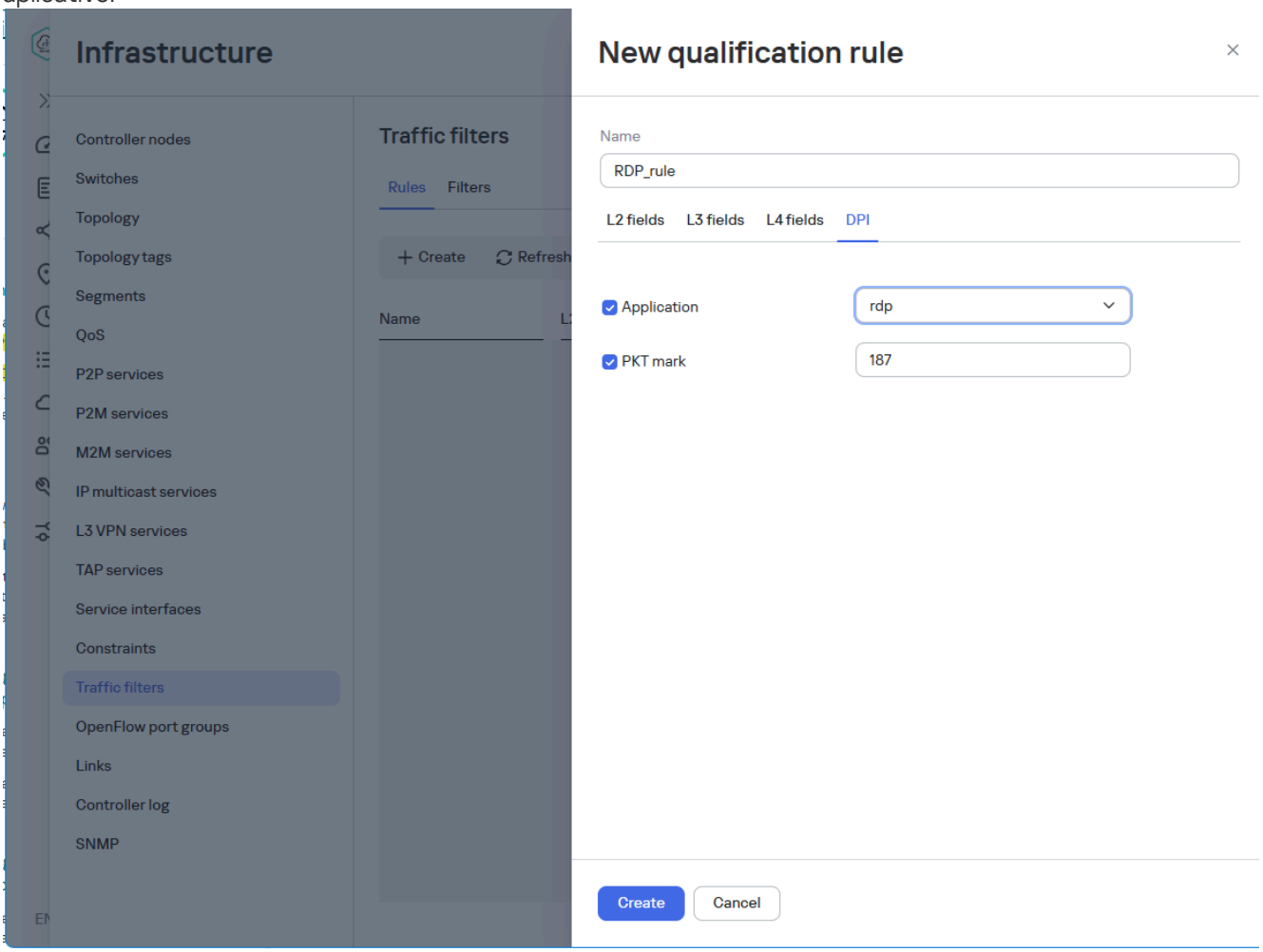
Começar a criar limites em um link de dispositivo CPE



Ativar o monitoramento de atraso e definir um nível de latência crítico

4. Criar uma regra de classificação de tráfego do aplicativo

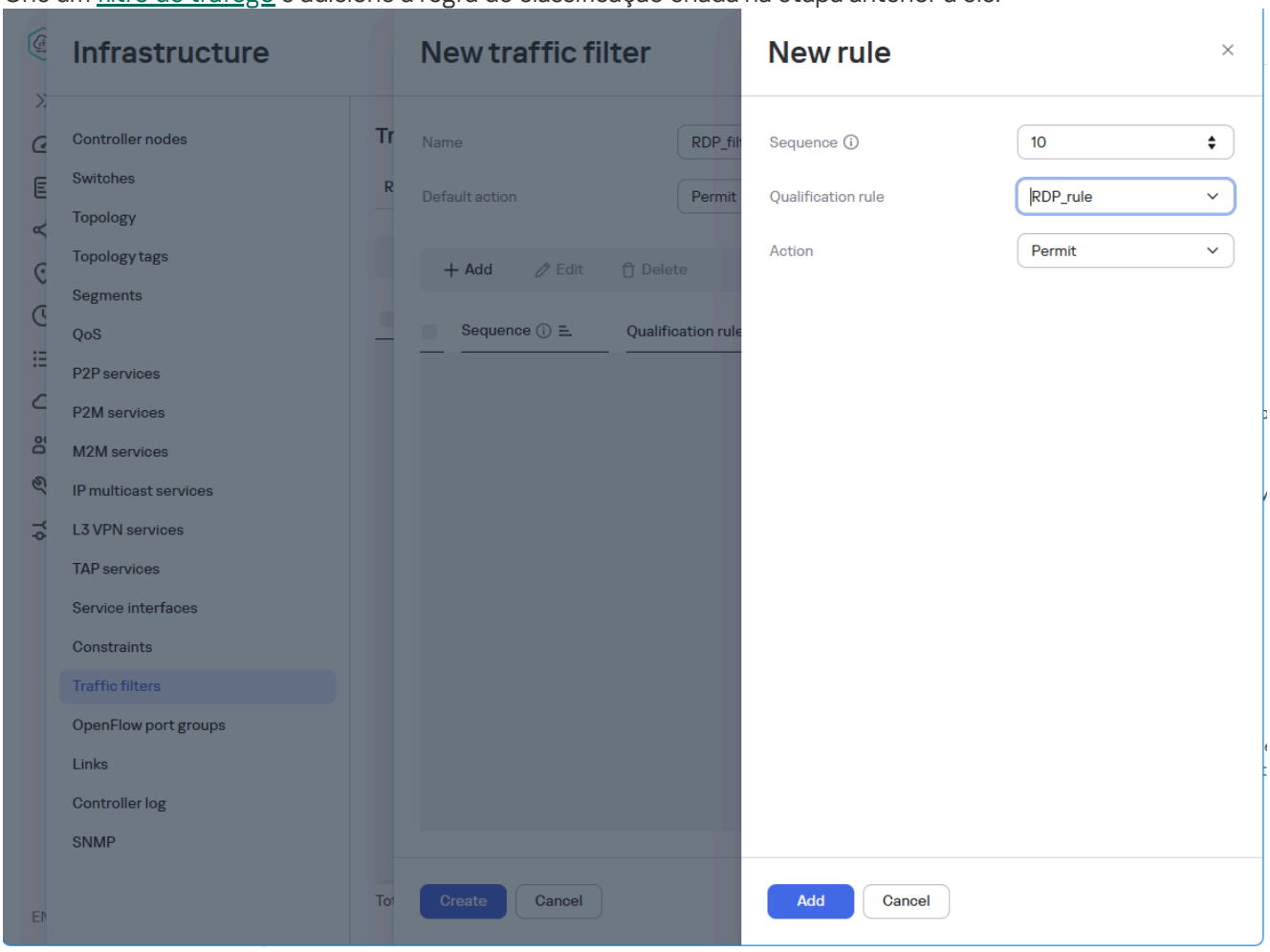
Para criar uma regra de classificação de tráfego, na guia **DPI**, especifique o valor de **dpi** para a classificação do aplicativo:



Criar uma regra de classificação de tráfego para o aplicativo RDP

5 Criar um filtro para identificar o tráfego do aplicativo

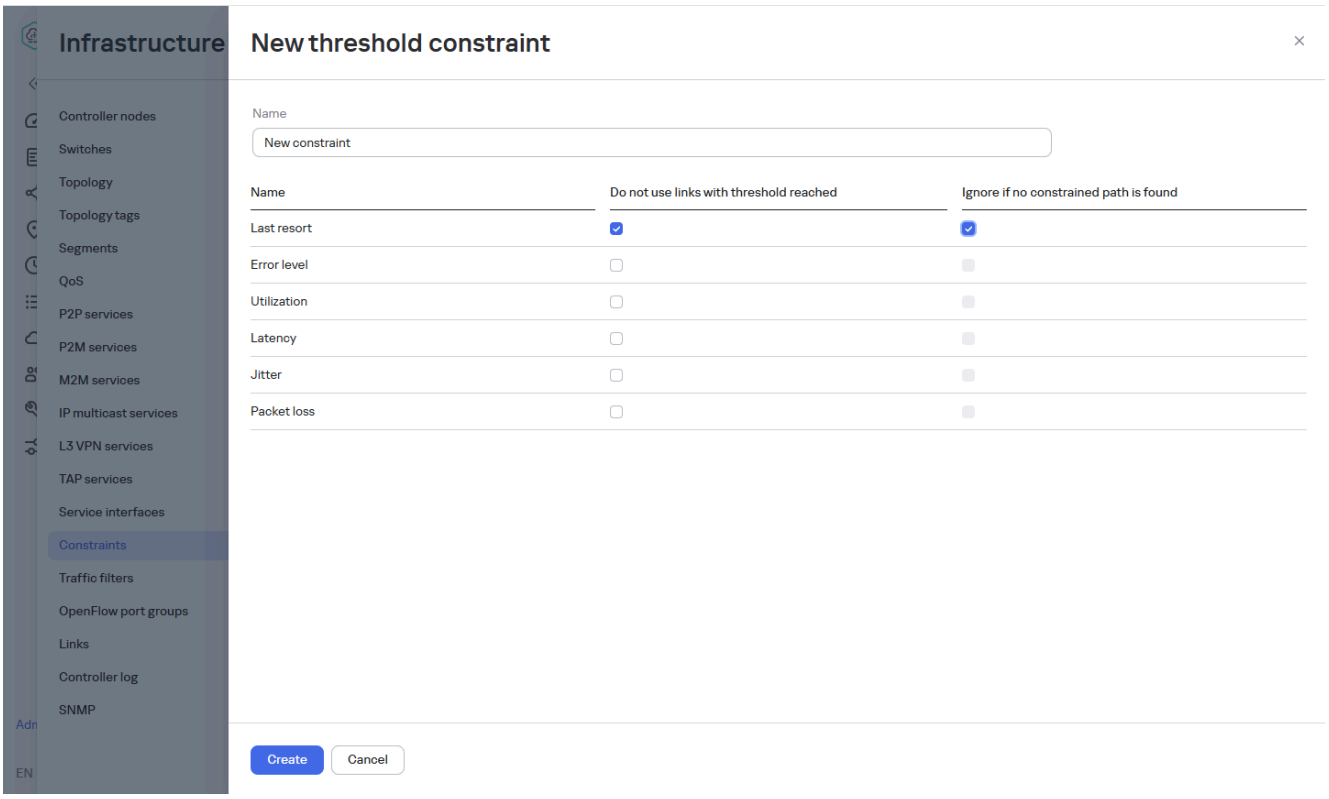
Crie um filtro de tráfego e adicione a regra de classificação criada na etapa anterior a ele:



Criar um filtro de tráfego

6 Criar restrições de limite

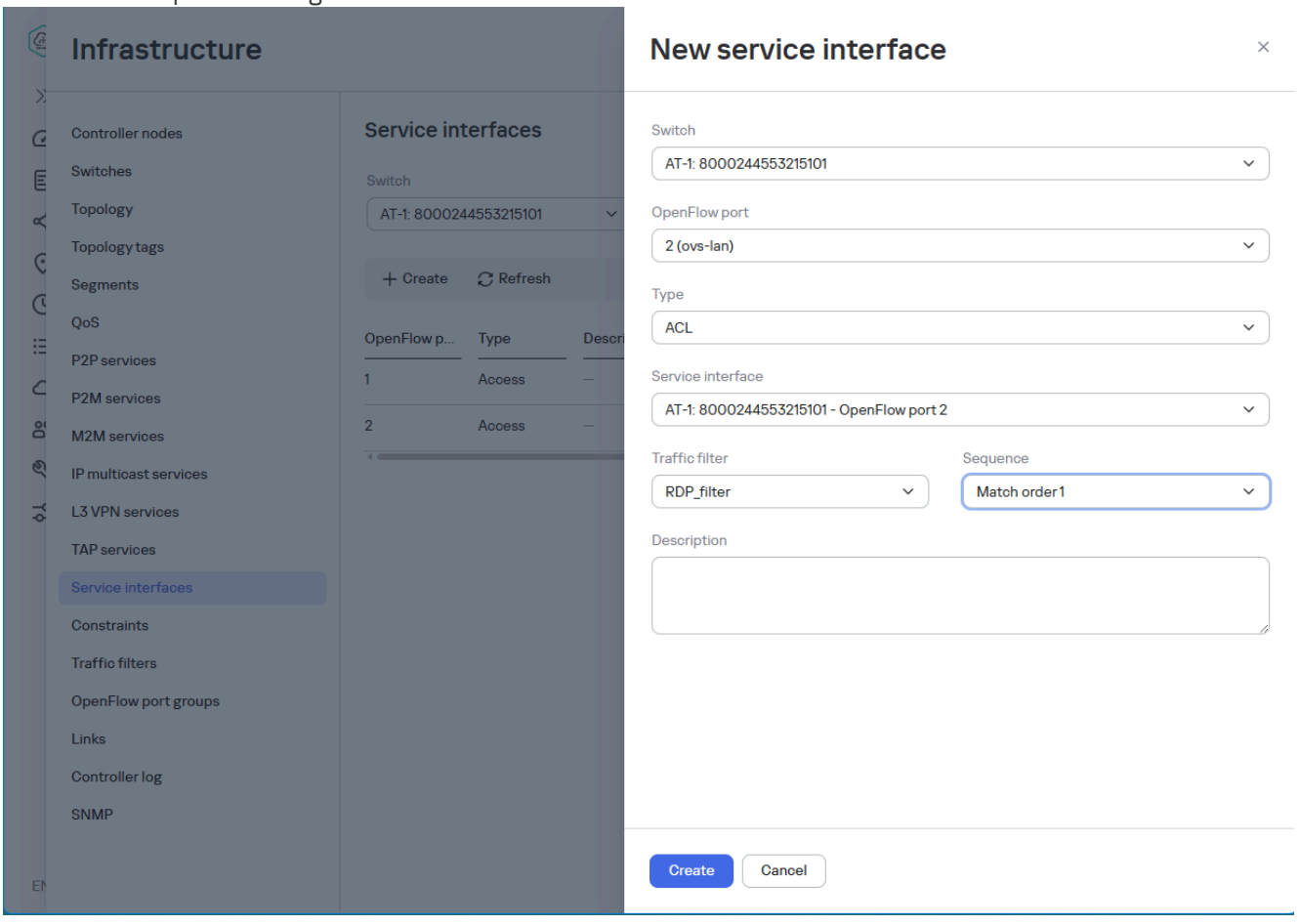
Crie uma restrição de limite para o controlador, selecione **Último recurso** como o indicador de monitoramento e marque ambas as caixas de seleção **Não usar links com limite alcançado** e **Ignorar se nenhum caminho restrito for encontrado**:



Criar um limite com o indicador de monitoramento "Último recurso"

7 Criar interfaces de serviço ACL

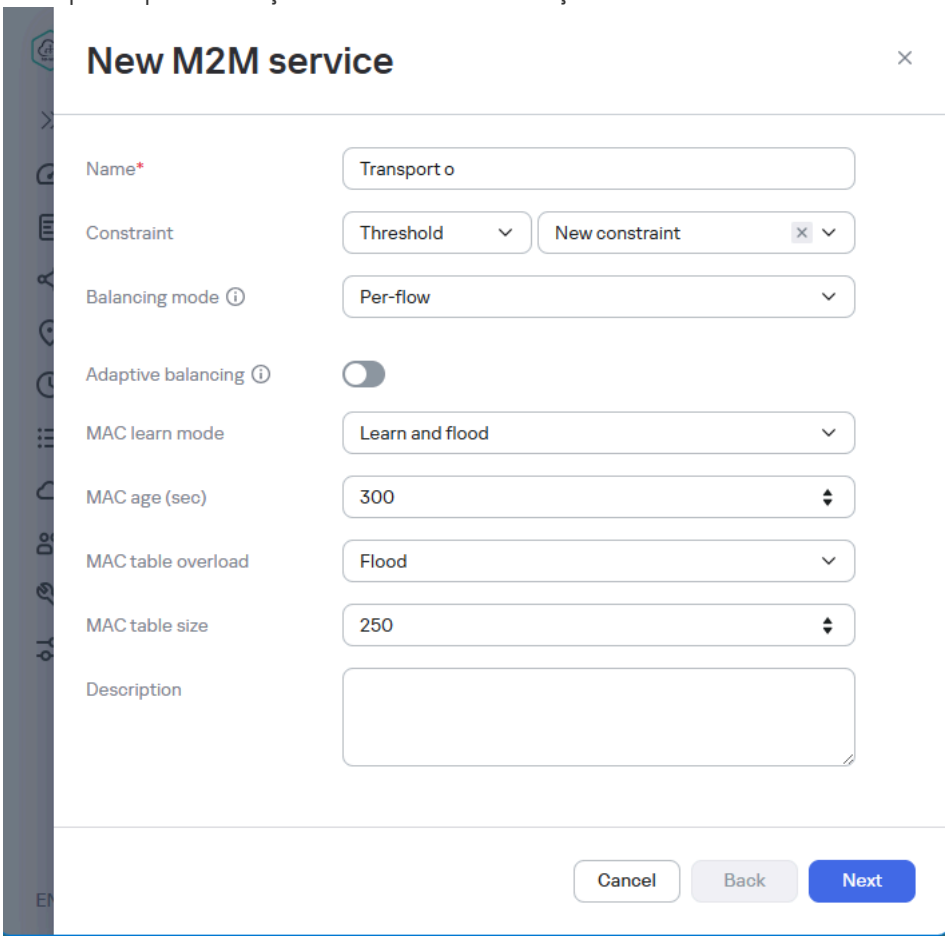
Crie interfaces de serviço do tipo ACL para o dispositivo CPE com a função de gateway e o dispositivo CPE padrão. Ao criar as interfaces, especifique a interface de serviço do serviço M2M principal e o filtro criado anteriormente para o tráfego RDP:



Adicionar uma interface ACL com o filtro de tráfego criado anteriormente

8 **Criar um serviço M2M separado**

Crie um serviço M2M que receberá somente tráfego RDP. Inclua nesse serviço apenas as interfaces ACL criadas na etapa anterior e especifique a restrição de limite "Nova restrição" criada anteriormente:



Adicionar um serviço M2M com uma restrição de limite

O tráfego RDP agora termina no novo serviço M2M. O restante do tráfego vai para a interface de serviço principal para ser distribuído entre os links disponíveis.

Gerenciar serviços de transporte ponto a ponto (P2P)

Para visualizar a tabela de serviços P2P, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Serviços P2P**. As informações sobre os serviços P2P são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do serviço P2P.
- **Origem** contém informações sobre a interface de serviço de origem do serviço P2P:
  - Nome e DPID do dispositivo CPE no qual a interface de serviço foi criada
  - O número da porta OpenFlow para a qual a interface de serviço é mapeada
- **Destino** contém informações sobre a interface de serviço de destino do serviço P2P:
  - Nome e DPID do dispositivo CPE no qual a interface de serviço foi criada
  - O número da porta OpenFlow para a qual a interface de serviço é mapeada

- **QoS** é a regra de qualidade de serviço especificada para a interface de serviço de origem do serviço P2P.
- **Interface de serviço de backup** contém informações sobre a interface de serviço de backup do serviço P2P:
  - Nome e DPID do dispositivo CPE no qual a interface de serviço foi criada
  - O número da porta OpenFlow para a qual a interface de serviço é mapeada
- **Status** é o status do serviço P2P:
  - **Para cima**
  - **Para baixo**

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um serviço P2P

Para criar um serviço P2P:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2P**.

   Uma tabela de serviços P2P é exibida.

4. Na parte superior da página, clique em **+ Serviço P2P**.

5. Na janela aberta, no campo **Nome**, insira o nome do serviço P2P.

6. Na lista suspensa **Restrição**, selecione a restrição Manual-TE criada ou a restrição de limite que deseja adicionar ao serviço P2P.

7. Na lista suspensa **Modo de balanceamento**, selecione o modo de balanceamento para a distribuição do tráfego entre os links:
   - **Por fluxo** significa que os fluxos de tráfego (5-Tuple) são distribuídos entre os links de acordo com o custo do link. Essa é a configuração padrão.
   - **Por pacote** significa que os pacotes de tráfego são distribuídos entre os links de acordo com o custo do link.
   - **Difusão** significa que os pacotes de tráfego são duplicados e transmitidos simultaneamente por todos os links para evitar perdas.

   É possível especificar o custo do link manualmente.

8. É possível configurar o modo de balanceamento adaptativo caso deseje que o peso do caminho seja ajustado dinamicamente dependendo do nível de perda de pacotes para o caminho:

    a. Ative o botão **Balanceamento adaptativo**.

    b. No campo **Índice mínimo de perda (%)**, especifique a porcentagem mínima de perda de pacotes no caminho na qual o balanceamento adaptativo começa para ajustar o peso. Intervalo de valores: 0,01 a 100.

    c. No campo **Índice máximo de perda (%)**, especifique a porcentagem máxima de perda de pacotes na qual o caminho é excluído do balanceamento de carga.

    d. Na lista suspensa **Velocidade de convergência**, selecione a taxa de convergência dos pesos adaptativos para os valores calculados:

    - **Rápido**: 1
    - **Rápido**: 0,75
    - **Rápido**: 0,5

9. Se necessário, no campo **Descrição**, insira uma breve descrição do serviço P2P.

10. Nas listas suspensas **Switch** e **Interface de serviço** à esquerda, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como interface de serviço de origem do serviço P2P.

11. Nas listas suspensas **Switch** e **Interface de serviço** à direita, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como interface de serviço de destino do serviço P2P.

12. Para exibir interfaces de serviço adicionadas aos serviços de transporte nas listas suspensas **Interface de serviço**, marque a caixa de seleção **Mostrar interfaces usadas**. Esta caixa de seleção está desmarcada por padrão.

13. Para trocar os valores selecionados nas listas suspensas **Interface de serviço**, marque a caixa de seleção **Interfaces de switch**. Esta caixa de seleção está desmarcada por padrão.

14. Para adicionar uma interface de serviço reserva da fonte de serviço P2P através da qual o tráfego é transmitido se a interface de serviço principal falhar:

    a. Marque a caixa de seleção **Usar interface de backup**. Esta caixa de seleção está desmarcada por padrão.

    b. Nas listas suspensas **Switch de backup** e**Interface de serviço de backup**, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como reserva.

    c. Para exibir interfaces de serviço adicionadas aos serviços de transporte, na lista suspensa **Interface de serviço de backup**, marque a caixa de seleção **Mostrar interfaces usadas**. Esta caixa de seleção está desmarcada por padrão.

    Se a interface do serviço de origem principal do serviço P2P for ativada novamente, o serviço P2P continuará usando a interface do serviço de origem reserva.

15. Nas listas suspensas **Filtro de entrada** à esquerda e à direita, selecione o filtro de tráfego criado para as interfaces de origem e destino do serviço P2P.

16. Na lista suspensa **QoS**, selecione a regra de qualidade de serviço criada para a interface de serviço da origem do serviço P2P.

17. Para rastrear o status das interfaces de serviço de origem e de destino do serviço P2P e, quando uma das interfaces ficar inativa, desativar automaticamente a outra, marque a caixa de seleção**Propagar status da interface**. Esta caixa de seleção está desmarcada por padrão. Essa caixa de seleção não pode ser marcada quando a caixa de seleção **Usar interface de backup**estiver marcada.

    Quando a interface de serviço desativada primeiro volta a ficar on-line, a segunda interface de serviço desativada automaticamente também retoma a operação. Essa funcionalidade funciona apenas em interfaces de serviço com classificação de tráfego de acesso. É possível selecionar o tipo de classificação de tráfego ao criar uma interface de serviço.

18. Clique em **Criar**.

O serviço P2P é criado e exibido na tabela.

Visualizar estatísticas de um serviço P2P

Para visualizar as estatísticas de um serviço P2P:

1. No menu, acesse a seção **Infraestrutura**.

    A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

    Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2P**.

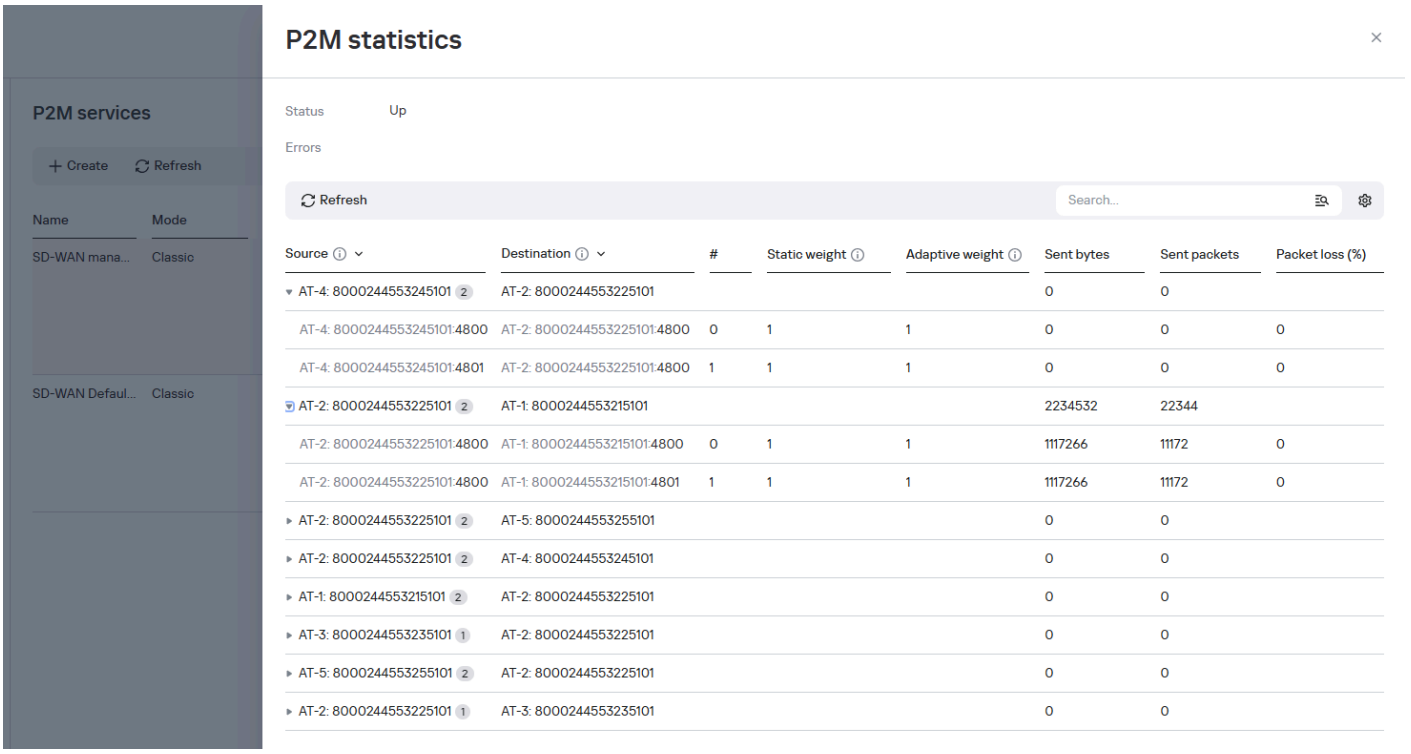
    Uma tabela de serviços P2P é exibida.

4. Clique em **Gerenciamento** → **Estatísticas** ao lado do serviço P2P cujas estatísticas deseja visualizar.

Isso abre uma janela com estatísticas do serviço P2P.

Na parte superior da janela de estatísticas, o campo **Status** exibe o status operacional do serviço. O campo **Erros** exibe possíveis erros que podem ocorrer para o serviço.

As estatísticas de segmentos, caminhos e links do serviço são exibidas hierarquicamente em uma tabela. As linhas da tabela são agrupadas por segmento. As linhas dentro de cada grupo contêm estatísticas dos caminhos incluídos no segmento correspondente. Para expandir um grupo, clique no triângulo (▸). Para serviços sem limites definidos, as linhas exibem todos os caminhos com balanceamento de carga ativado no segmento. Para serviços com limites, as linhas exibem os caminhos de Auto-TE que atendem aos limites.



Exibição de estatísticas usando um serviço P2M como exemplo

As informações estatísticas detalhadas sobre segmentos e caminhos são exibidas nas seguintes colunas da tabela:

Origem: para linhas agregadas, o host de origem do segmento; para linhas em grupos expansíveis, o host de origem do caminho no segmento.

Destino: para linhas agregadas, o host de destino do segmento; para linhas em grupos expansíveis, o host de destino do caminho no segmento.

é o número sequencial do caminho. Quanto menor o número do caminho, há mais tempo ele foi criado. Esse valor é exibido apenas nas linhas em grupos expansíveis.

Peso estático é o peso do caminho estático com base no custo. Esse valor é exibido apenas para linhas em grupos expansíveis.

Peso adaptativo é o peso dinâmico do caminho com base na análise da perda de pacotes nesse caminho. Esse valor é exibido apenas para linhas em grupos expansíveis. Se o balanceamento adaptativo não for usado, essa coluna não é exibida.

Bytes enviados: para linhas agregadas, o valor da janela de estatísticas do serviço atual; para linhas em grupos expansíveis, o número de bytes enviados ao bucket do grupo OF.

Pacotes enviados: para linhas agregadas, o valor da janela de estatísticas do serviço atual; para linhas em grupos expansíveis, o número de pacotes enviados ao bucket do grupo OF.

Perda de pacotes (%) é a porcentagem de perda de pacotes em um determinado caminho (a razão entre o número de pacotes perdidos e o número total de pacotes enviados). Esse valor é exibido apenas nas linhas em grupos expansíveis.

Visualizar e configurar a exibição de uma topologia de serviço P2P

Para visualizar e configurar a exibição de uma topologia de serviço P2P:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2P**.

   Uma tabela de serviços P2P é exibida.

4. Clique em **Gerenciamento** → **Topologia de serviço** ao lado do serviço P2P cuja topologia deseja visualizar.

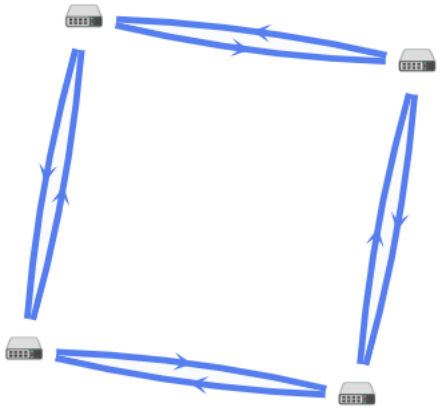
   Isso abre uma janela com a topologia do serviço P2P.

5. Caso seja necessário mover dispositivos CPE, execute uma das seguintes ações:

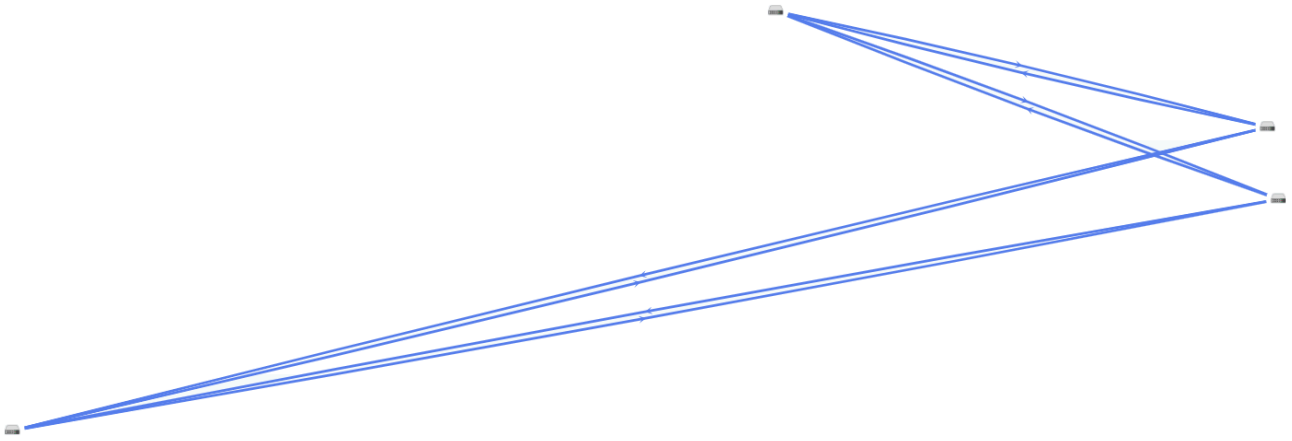
   - Para alterar manualmente a posição dos dispositivos CPE, clique em **Manual** e ajuste a posição dos dispositivos.

   - Para organizar dispositivos CPE automaticamente, clique em **Automaticamente** e selecione um dos seguintes valores na lista suspensa exibida:

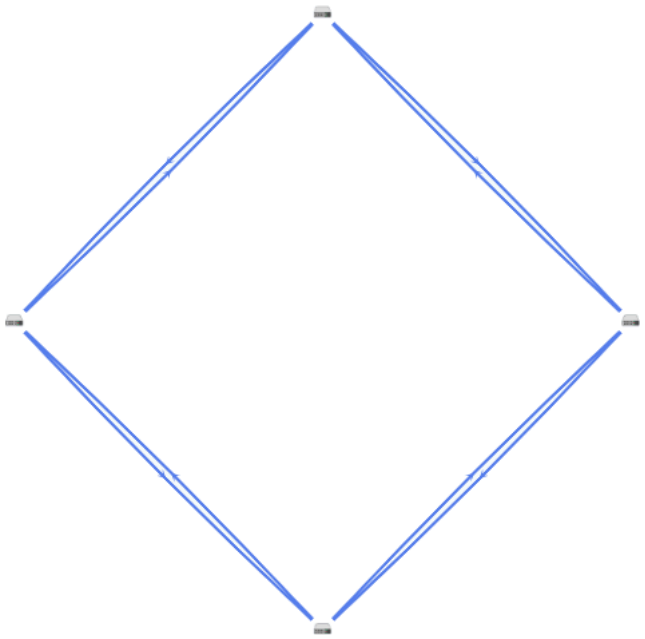
     - **Simulação física** — Os dispositivos CPE são organizados aproximadamente de acordo com sua localização real em relação uns aos outros, por exemplo:



- **Aleatório** — A organização dos dispositivos CPE é aleatória, por exemplo:

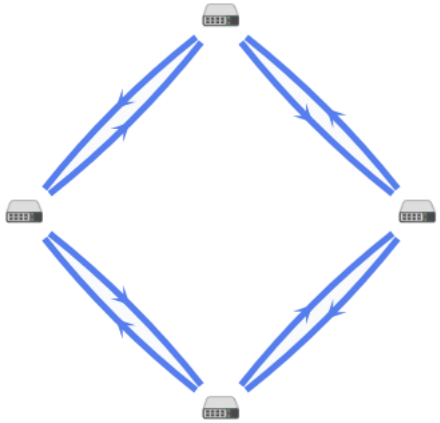


- **Círculo** — Os dispositivos CPE são organizados de acordo com uma topologia em anel, por exemplo:



- **Em largura** — Os dispositivos CPE são organizados horizontalmente, por exemplo:

- **Concêntrico** — Os dispositivos CPE são organizados de forma concêntrica, por exemplo:



- **Grade** — Os dispositivos CPE são organizados de acordo com uma topologia de grade, por exemplo:

6. Para exibir informações sobre dispositivos CPE, marque as seguintes caixas de seleção:

   - **Nome** exibe os nomes dos dispositivos CPE.
   - **Endereço IP** exibe os endereços IP dos dispositivos CPE.

   Essas caixas de seleção são desmarcadas por padrão.

7. Para exibir um segmento entre dois dispositivos CPE:

   a. Marque a caixa de seleção **Segmentos**. Esta caixa de seleção está desmarcada por padrão.

   b. Nas listas suspensas exibidas, selecione os dispositivos CPE de origem e destino do segmento.

   O segmento entre os dispositivos CPE é exibido.

Editar um serviço P2P

Para editar um serviço P2P:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2P**.

   Uma tabela de serviços P2P é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do serviço P2P que deseja editar.

5. Na janela aberta, se necessário, edite as configurações do serviço P2P. Para obter uma descrição das configurações, consulte as instruções para criar um serviço P2P.

6. Clique em **Salvar**.

O serviço P2P é modificado e atualizado na tabela.

Reiniciar um serviço P2P

É possível reiniciar um serviço P2P para restaurá-lo em caso de mau funcionamento. Ao reiniciar um serviço P2P, o controlador exclui e recria automaticamente as regras associadas ao serviço P2P nas tabelas OpenFlow dos dispositivos CPE. Isso afeta os dispositivos CPE cujas interfaces de serviço são adicionadas ao serviço P2P.

Para reiniciar um serviço P2P:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2P**.

   Uma tabela de serviços P2P é exibida.

4. Clique em **Gerenciamento** → **Reaprovisionamento** ao lado do serviço P2P que deseja reprovisionar.

5. Na janela de confirmação, clique em **Reaprovisionamento**.

O serviço P2P é reiniciado.

Excluir um serviço P2P

Os serviços P2P excluídos não podem ser restaurados

Para excluir um serviço P2P:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2P**.

   Uma tabela de serviços P2P é exibida.

4. Clique em **Gerenciamento** → **Excluir** ao lado do serviço P2P que deseja excluir.

5. Para excluir as interfaces de serviço adicionadas ao serviço P2P, marque a caixa de seleção **Excluir interfaces de serviço associadas** na janela de confirmação. Esta caixa de seleção está desmarcada por padrão.

6. Clique em **Excluir**.

O serviço P2P é excluído e não é mais exibido na tabela.

Gerenciar serviços de transporte ponto a multiponto (P2M)

Para visualizar a tabela de serviços P2M, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Serviços P2M**. As informações sobre os serviços P2M são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do serviço P2M.
- **Modo** indica se uma DFI (Interface de encaminhamento padrão) é usada no serviço P2M para o qual o tráfego unicast desconhecido é enviado:
  - **Clássico** caso não deseje usar uma DFI. Essa é a configuração padrão.
  - **DFI com FIB na raiz e folhas** para usar uma DFI na interface de serviço com a função raiz.
  - **DFI com FIB na folha** para usar uma DFI na interface de serviço com a função raiz. As interfaces de serviço com a função folha devem ser criadas no mesmo dispositivo CPE. As interfaces de serviço de backup com a função folha devem ser criadas no mesmo dispositivo CPE, que deve ser diferente do dispositivo CPE no qual as interfaces de serviço principais foram criadas.
- **Idade do MAC (s)** é o tempo, em segundos, durante o qual as entradas são mantidas na tabela MAC do controlador.
- **Modo de aprendizado MAC** é a ação aplicada a uma série de quadros quando o primeiro quadro é enviado ao controlador para aprender o endereço MAC de origem:
  - **Aprender e inundar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros será enviada para todas as interfaces de serviço adicionadas ao serviço P2M, exceto para a interface de serviço na qual a série de quadros chegou originalmente.
  - **Aprender e descartar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros é descartada.

  Se o endereço MAC de destino estiver presente na tabela MAC, a série de quadros é enviada para a interface de serviço de destino.
- **Tamanho da tabela MAC** é o número máximo de entradas na tabela MAC no controlador.
- **Sobrecarga da tabela MAC** é a política de processamento de novos endereços MAC quando a tabela MAC do controlador está cheia:
  - **Inundação** significa que o tráfego com endereços MAC de destino que não foram aprendidos é transmitido como tráfego BUM (broadcast, unknown-unicast e multicast).
  - **Descartar** significa que o tráfego com endereços MAC de destino que não foram aprendidos é descartado.

- **Endpoints** são as informações sobre as interfaces de serviço adicionadas ao serviço P2M:
  - Nomes e DPIDs dos dispositivos CPE nos quais as interfaces de serviço foram criadas
  - Números de portas OpenFlow para as quais as interfaces de serviço são mapeadas
  - Funções das interfaces de serviço:
    - **Raiz** significa que a interface de serviço pode enviar tráfego para interfaces de serviço com qualquer função.
    - **Folha** significa que a interface de serviço pode enviar tráfego apenas para interfaces de serviço com a função **Raiz**.
- **Status** é o status do serviço P2M:
  - **Para cima**
  - **Para baixo**
- **Descrição** é uma breve descrição do serviço P2M.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um serviço P2M

Para criar um serviço P2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, você é levado à seção **Nós do controlador**, que exibe uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2M**.

   Uma tabela de serviços P2M é exibida.

4. Na parte superior da página, clique em **+ Serviço P2M**.

5. Na janela aberta, no campo **Nome**, insira o nome do serviço P2M.

6. Na lista suspensa **Restrição**, selecione a restrição Manual-TE criada ou a restrição de limite que deseja adicionar ao serviço P2M.

7. Na lista suspensa **Modo de balanceamento**, selecione o modo de balanceamento para a distribuição do tráfego entre os links:

   - **Por fluxo** significa que os fluxos de tráfego (5-Tuple) são distribuídos entre os links de acordo com o custo do link. Essa é a configuração padrão.
   - **Por pacote** significa que os pacotes de tráfego são distribuídos entre os links de acordo com o custo do link.
   - **Difusão** significa que os pacotes de tráfego são duplicados e transmitidos simultaneamente por todos os links para evitar perdas.

   É possível especificar o custo do link manualmente.

8. É possível configurar o modo de balanceamento adaptativo caso deseje que o peso do caminho seja ajustado dinamicamente dependendo do nível de perda de pacotes para o caminho:

   a. Ative o botão **Balanceamento adaptativo**.

   b. No campo **Índice mínimo de perda (%)**, especifique a porcentagem mínima de perda de pacotes no caminho na qual o balanceamento adaptativo começa para ajustar o peso. Intervalo de valores: 0,01 a 100.

   c. No campo **Índice máximo de perda (%)**, especifique a porcentagem máxima de perda de pacotes na qual o caminho é excluído do balanceamento de carga.

   d. Na lista suspensa **Velocidade de convergência**, selecione a taxa de convergência dos pesos adaptativos para os valores calculados:

      - **Rápido**: 1
      - **Rápido**: 0,75
      - **Rápido**: 0,5

9. Na lista suspensa **Modo**, selecione se o serviço P2M usa uma DFI (Interface de encaminhamento padrão), para a qual o tráfego unicast desconhecido é enviado:

   - **Clássico** caso não deseje usar uma DFI. Essa é a configuração padrão.
   - **DFI com FIB na raiz e folhas** para usar uma DFI na interface de serviço com a função raiz.
   - **DFI com FIB na folha** para usar uma DFI na interface de serviço com a função raiz. As interfaces de serviço com a função folha devem ser criadas no mesmo dispositivo CPE. As interfaces de serviço de backup com a função folha devem ser criadas no mesmo dispositivo CPE, que deve ser diferente do dispositivo CPE no qual as interfaces de serviço principais foram criadas.

10. Na lista suspensa **Modo de aprendizado MAC**, selecione a ação que deseja aplicar a uma série de quadros quando o primeiro for enviado ao controlador para saber o endereço MAC de origem:

    - **Aprender e inundar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros será enviada para todas as interfaces de serviço adicionadas ao serviço P2M, exceto para a interface de serviço na qual a série de quadros chegou originalmente. Essa é a configuração padrão.

    - **Aprender e descartar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros é descartada.

    Se o endereço MAC de destino estiver presente na tabela MAC, a série de quadros é enviada para a interface de serviço de destino.

11. No campo **Idade do MAC (s)**, insira o tempo (em segundos) durante o qual as entradas são mantidas na tabela MAC do controlador. Intervalo de valores: 10 a 65.535. O valor padrão é `300`.

12. Na lista suspensa **Sobrecarga da tabela MAC**, selecione a política de processamento de novos endereços MAC quando a tabela MAC do controlador está cheia:

    - **Inundação** significa que o tráfego com endereços MAC de destino que não foram aprendidos é transmitido como tráfego BUM (broadcast, unknown-unicast e multicast). Essa é a configuração padrão.

    - **Descartar** significa que o tráfego com endereços MAC de destino que não foram aprendidos é descartado.

13. No campo **Tamanho da tabela MAC**, insira o número máximo de entradas na tabela MAC no controlador. Intervalo de valores: 0 a 65.535. `0` significa que o número de registros na tabela MAC do controlador não é limitado. O valor padrão é `100`.

14. Se necessário, no campo **Descrição**, insira uma breve descrição do serviço P2M.

15. Clique em **Next** para prosseguir para o próximo grupo de configurações.

16. Adicione a interface de serviço ao serviço P2M:

    a. Clique em **+ Adicionar**.

    As configurações da interface de serviço são exibidas.

    b. Nas listas suspensas **Switch** e **Interface de serviço** à direita, selecione o dispositivo CPE e a interface de serviço criada que deseja adicionar ao serviço P2M.

    c. Na lista suspensa **QoS**, selecione a regra de qualidade de serviço criada para a interface de serviço.

    d. Na lista suspensa **Filtro de entrada**, selecione o filtro de tráfego criado para a interface de serviço.

    e. Na lista suspensa **Função**, selecione a função da interface de serviço:

    - **Raiz** significa que a interface de serviço pode enviar tráfego para interfaces de serviço com qualquer função.

    - **Folha** significa que a interface de serviço pode enviar tráfego apenas para interfaces de serviço com a função **Raiz**.

    - **Raiz, interface de encaminhamento padrão**significa que a interface de serviço pode enviar tráfego para interfaces de serviço com qualquer função, e a função DFI está atribuída a essa interface de serviço.

f. Para adicionar uma interface de serviço de backup através da qual o tráfego deve ser enviado quando a interface de serviço principal falhar, nas listas suspensas **Switch de backup** e **Interface de serviço de backup**, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como interface de serviço de backup.

Se a interface de serviço principal voltar a ficar on-line, o serviço P2M continua a usar a interface de serviço de backup.

A interface de serviço é adicionada e exibida na parte inferior da janela. É possível adicionar várias interfaces de serviço ou excluir interfaces de serviço. Para excluir uma interface de serviço, clique no ícone de exclusão ✕ ao lado dela.

17. Clique em **Next** para prosseguir para o próximo grupo de configurações.

18. Para adicionar várias interfaces de rede a um serviço P2M ao mesmo tempo, adicione um grupo de portas OpenFlow. Para isso, execute as seguintes ações:

a. Clique em **+ Adicionar**.

As configurações do grupo de portas OpenFlow são exibidas.

b. Na lista suspensa **Grupo**, selecione o grupo de portas OpenFlow criado que deseja adicionar ao serviço P2M. Ao salvar as configurações do serviço P2M, interfaces de serviço são criadas automaticamente e mapeadas para portas OpenFlow no grupo OpenFlow; em seguida, essas interfaces de serviço são adicionadas automaticamente ao serviço P2M.

c. Na lista suspensa **QoS**, selecione a regra de qualidade de serviço criada para interfaces de serviço criadas automaticamente e mapeadas para portas OpenFlow.

d. No campo **ID da VLAN**, insira o valor da tag de VLAN externa para interfaces de serviço criadas automaticamente e mapeadas para portas OpenFlow. As interfaces de serviço do tipo classificação de tráfego VLAN só podem ser criadas automaticamente. A mesma tag de VLAN externa é atribuída a cada interface de serviço.

e. Na lista suspensa **Função**, selecione a função para interfaces de serviço criadas automaticamente e mapeadas para portas OpenFlow:

- **Raiz** significa que a interface de serviço pode enviar tráfego para interfaces de serviço com qualquer função.
- **Folha** significa que a interface de serviço pode enviar tráfego apenas para interfaces de serviço com a função **Raiz**.

O grupo OpenFlow é adicionado e exibido na parte inferior da janela. É possível adicionar vários grupos de portas OpenFlow ou excluir grupos de portas OpenFlow. Para excluir um grupo de portas OpenFlow, clique no ícone de exclusão ✕ ao lado dele.

19. Clique em **Criar**.

O serviço P2M é criado e exibido na tabela.

Visualizar estatísticas de um serviço P2M

Para visualizar as estatísticas de um serviço P2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, você é levado à seção **Nós do controlador**, que exibe uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2M**.

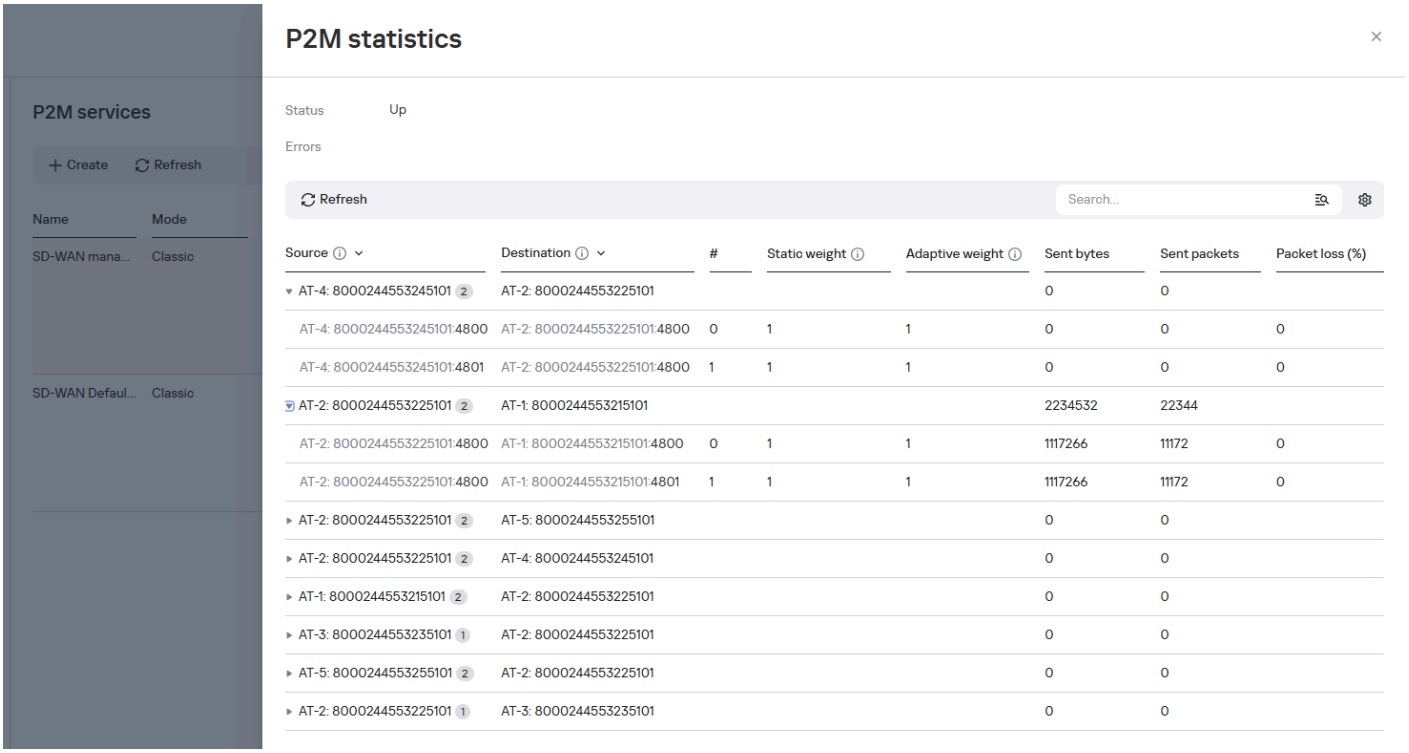
   Uma tabela de serviços P2M é exibida.

4. Clique em **Gerenciamento** → **Estatísticas** ao lado do serviço P2M cujas estatísticas deseja visualizar.

Isso abre uma janela com estatísticas do serviço P2M.

Na parte superior da janela de estatísticas, o campo **Status** exibe o status operacional do serviço. O campo **Erros** exibe possíveis erros que podem ocorrer para o serviço.

As estatísticas de segmentos, caminhos e links do serviço são exibidas hierarquicamente em uma tabela. As linhas da tabela são agrupadas por segmento. As linhas dentro de cada grupo contêm estatísticas dos caminhos incluídos no segmento correspondente. Para expandir um grupo, clique no triângulo (▸). Para serviços sem limites definidos, as linhas exibem todos os caminhos com balanceamento de carga ativado no segmento. Para serviços com limites, as linhas exibem os caminhos de Auto-TE que atendem aos limites.



Exibição de estatísticas usando um serviço P2M como exemplo

As informações estatísticas detalhadas sobre segmentos e caminhos são exibidas nas seguintes colunas da tabela:

Origem: para linhas agregadas, o host de origem do segmento; para linhas em grupos expansíveis, o host de origem do caminho no segmento.

Destino: para linhas agregadas, o host de destino do segmento; para linhas em grupos expansíveis, o host de destino do caminho no segmento.

é o número sequencial do caminho. Quanto menor o número do caminho, há mais tempo ele foi criado. Esse valor é exibido apenas nas linhas em grupos expansíveis.

Peso estático é o peso do caminho estático com base no custo. Esse valor é exibido apenas para linhas em grupos expansíveis.

Peso adaptativo é o peso dinâmico do caminho com base na análise da perda de pacotes nesse caminho. Esse valor é exibido apenas para linhas em grupos expansíveis. Se o balanceamento adaptativo não for usado, essa coluna não é exibida.

Bytes enviados: para linhas agregadas, o valor da janela de estatísticas do serviço atual; para linhas em grupos expansíveis, o número de bytes enviados ao bucket do grupo OF.

Pacotes enviados: para linhas agregadas, o valor da janela de estatísticas do serviço atual; para linhas em grupos expansíveis, o número de pacotes enviados ao bucket do grupo OF.

Perda de pacotes (%) é a porcentagem de perda de pacotes em um determinado caminho (a razão entre o número de pacotes perdidos e o número total de pacotes enviados). Esse valor é exibido apenas nas linhas em grupos expansíveis.

Visualizar a tabela MAC de um serviço P2M

Para visualizar a tabela MAC de um serviço P2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, você é levado à seção **Nós do controlador**, que exibe uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2M**.

   Uma tabela de serviços P2M é exibida.

4. Clique e, **Gerenciamento** → **Tabela MAC** ao lado do serviço P2M cuja tabela MAC você deseja visualizar.

Isso abre uma janela com a tabela MAC do serviço P2M. As informações sobre os endereços MAC são exibidas nas seguintes colunas da tabela:

- **MAC** é o endereço MAC.
- **Nome do host** é o DPID do switch onde está localizado o endereço MAC.
- **Porta** é o número da porta onde está localizado o endereço MAC.
- **VLAN** é o segmento da VLAN onde está localizado o endereço MAC.
- **Idade (s)** é o tempo em segundos durante o qual o endereço MAC esteve presente na tabela de endereços MAC.

5. Para encontrar um endereço MAC específico, insira-o no campo e clique em **Encontrar pelo MAC**.
6. Para limpar a tabela MAC, clique em **Limpar**.

Visualizar e configurar a exibição de uma topologia de serviço P2M

Para visualizar e configurar a exibição de uma topologia de serviço P2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, você é levado à seção **Nós do controlador**, que exibe uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2M**.

   Uma tabela de serviços P2M é exibida.

4. Clique em **Gerenciamento** → **Topologia de serviço** ao lado do serviço P2M cuja topologia deseja visualizar.

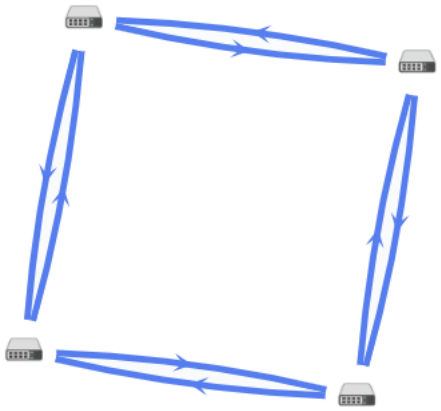
   Isso abre uma janela com a topologia do serviço P2M.

5. Caso seja necessário migrar dispositivos CPE, execute uma das seguintes ações:

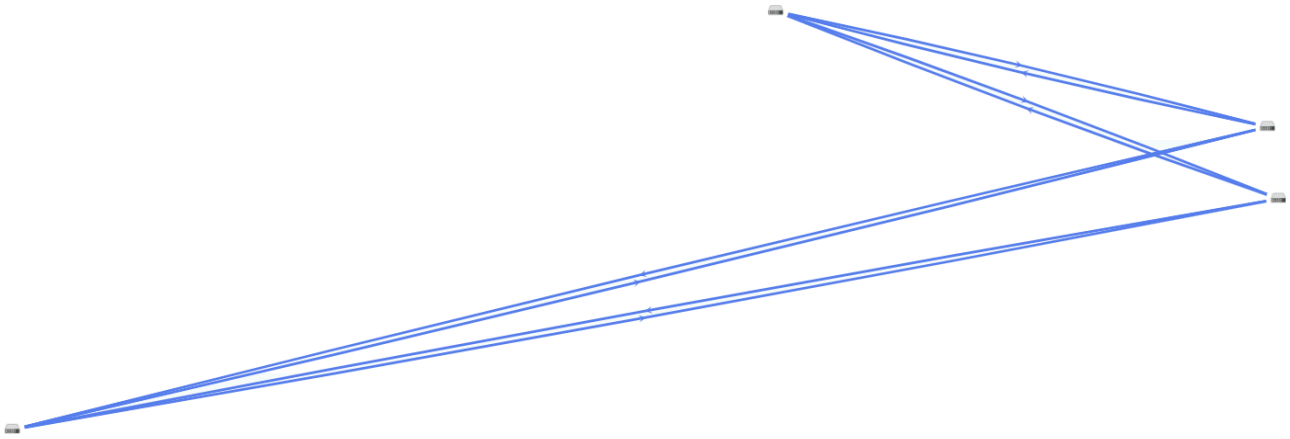
- Para alterar manualmente a posição dos dispositivos CPE, clique em **Manual** e ajuste a posição dos dispositivos.

- Para organizar dispositivos CPE automaticamente, clique em **Automaticamente** e selecione um dos seguintes valores na lista suspensa exibida:

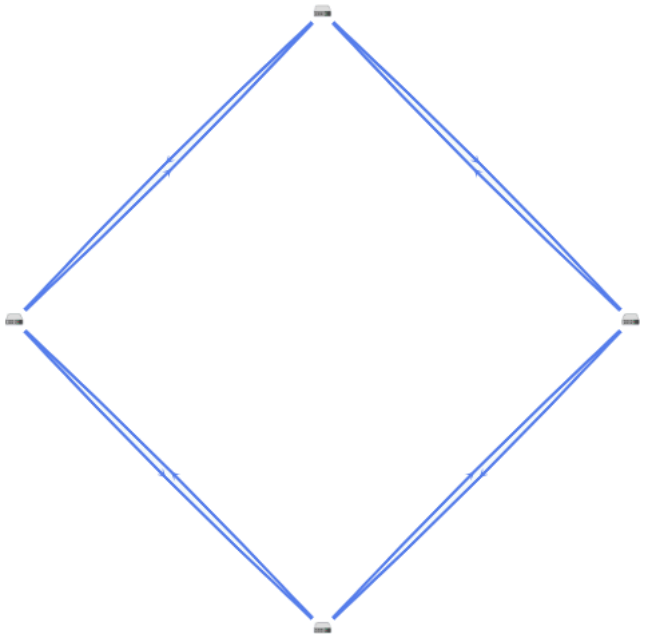
  - **Simulação física** — Os dispositivos CPE são organizados aproximadamente de acordo com sua localização real em relação uns aos outros, por exemplo:



  - **Aleatório** — A organização dos dispositivos CPE é aleatória, por exemplo:

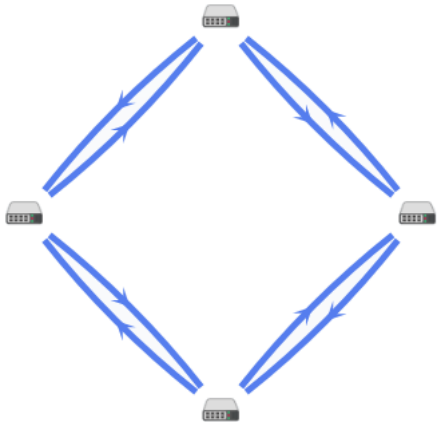


  - **Círculo** — Os dispositivos CPE são organizados de acordo com uma topologia em anel, por exemplo:



- **Em largura** — Os dispositivos CPE são organizados horizontalmente, por exemplo:

- **Concêntrico** — Os dispositivos CPE são organizados de forma concêntrica, por exemplo:



- **Grade** — Os dispositivos CPE são organizados de acordo com uma topologia de grade, por exemplo:

6. Para exibir informações sobre dispositivos CPE, marque as seguintes caixas de seleção:

   - **Nome** exibe os nomes dos dispositivos CPE.
   - **Endereço IP** exibe os endereços IP dos dispositivos CPE.

   Essas caixas de seleção são desmarcadas por padrão.

7. Para exibir um segmento entre dois dispositivos CPE:

   a. Marque a caixa de seleção **Segmentos**. Esta caixa de seleção está desmarcada por padrão.

   b. Nas listas suspensas exibidas, selecione os dispositivos CPE de origem e destino do segmento.

   O segmento entre os dispositivos CPE é exibido.

Editar um serviço P2M

Para editar um serviço P2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, você é levado à seção **Nós do controlador**, que exibe uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2M**.

   Uma tabela de serviços P2M é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do serviço P2M que deseja editar.

5. Na janela aberta, se necessário, edite as configurações do serviço P2M. Para obter uma descrição das configurações, consulte as instruções para criar um serviço P2M.

6. Clique em **Salvar**.

O serviço P2M é modificado e atualizado na tabela.

Reiniciar um serviço P2M

É possível reiniciar um serviço P2M para restaurá-lo em caso de mau funcionamento. Ao reiniciar um serviço P2M, o controlador exclui e recria automaticamente as regras associadas ao serviço P2M nas tabelas OpenFlow dos dispositivos CPE. Isso afeta os dispositivos CPE cujas interfaces de serviço são adicionadas ao serviço P2M.

Para reiniciar um serviço P2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, você é levado à seção **Nós do controlador**, que exibe uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2M**.

   Uma tabela de serviços P2M é exibida.

4. Clique em **Gerenciamento** → **Reaprovisionamento** ao lado do serviço P2M que deseja reprovisionar.

5. Na janela de confirmação, clique em **Confirmar**.

O serviço P2M é reiniciado.

Excluir um serviço P2M

Os serviços P2M excluídos não podem ser restaurados.

Para excluir um serviço P2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, você é levado à seção **Nós do controlador**, que exibe uma tabela de nós do controlador.

3. Vá para a seção **Serviços P2M**.

   Uma tabela de serviços P2M é exibida.

4. Clique em **Gerenciamento** → **Excluir** ao lado do serviço P2M que deseja excluir.

5. Para excluir as interfaces de serviço adicionadas ao serviço P2M, marque a caixa de seleção **Excluir interfaces de serviço associadas** na janela de confirmação. Esta caixa de seleção está desmarcada por padrão.

6. Clique em **Excluir**.

O serviço P2M é excluído e não é mais exibido na tabela.

Gerenciar serviços de transporte multiponto a multiponto (M2M)

Para visualizar a tabela de serviços M2M, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Serviços M2M**. As informações sobre os serviços M2M são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do serviço M2M.
- **Idade do MAC (s)** é o tempo, em segundos, durante o qual as entradas são mantidas na tabela MAC do controlador.
- **Modo de aprendizado MAC** é a ação aplicada a uma série de quadros quando o primeiro quadro é enviado ao controlador para aprender o endereço MAC de origem:
  - **Aprender e inundar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros será enviada a todas as interfaces de serviço adicionadas ao serviço M2M, exceto à interface de serviço na qual a série de quadros chegou originalmente.
  - **Aprender e descartar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros é descartada.

  Se o endereço MAC de destino estiver presente na tabela MAC, a série de quadros é enviada para a interface de serviço de destino.
- **Tamanho da tabela MAC** é o número máximo de entradas na tabela MAC no controlador.
- **Sobrecarga da tabela MAC** é a política de processamento de novos endereços MAC quando a tabela MAC do controlador está cheia:
  - **Inundação** significa que o tráfego com endereços MAC de destino que não foram aprendidos é transmitido como tráfego BUM (broadcast, unknown-unicast e multicast). Essa é a configuração padrão.
  - **Descartar** significa que o tráfego com endereços MAC de destino que não foram aprendidos é descartado.

- **Endpoints** são as informações sobre as interfaces de serviço adicionadas ao serviço M2M:
  - Nomes e DPIDs dos dispositivos CPE nos quais as interfaces de serviço foram criadas
  - Números de portas OpenFlow para as quais as interfaces de serviço são mapeadas
  - Funções das interfaces de serviço
- **Status** é o status do serviço M2M:
  - **Para cima**
  - **Para baixo**
- **Descrição** é uma breve descrição do serviço M2M.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um serviço M2M

Para criar um serviço M2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços M2M**.

   Uma tabela de serviços M2M é exibida.

4. Na parte superior da página, clique em **+ Serviço M2M**.

5. Na janela aberta, no campo **Nome**, insira o nome do serviço M2M.

6. Na lista suspensa **Restrição**, selecione a restrição Manual-TE criada ou a restrição de limite que deseja adicionar ao serviço M2M.

7. Na lista suspensa **Modo de balanceamento**, selecione o modo de balanceamento para a distribuição do tráfego entre os links:
   - **Por fluxo** significa que os fluxos de tráfego (5-Tuple) são distribuídos entre os links de acordo com o custo do link. Essa é a configuração padrão.
   - **Por pacote** significa que os pacotes de tráfego são distribuídos entre os links de acordo com o custo do link.
   - **Difusão** significa que os pacotes de tráfego são duplicados e transmitidos simultaneamente por todos os links para evitar perdas.

É possível especificar o custo do link manualmente.

8. É possível configurar o modo de balanceamento adaptativo caso deseje que o peso do caminho seja ajustado dinamicamente dependendo do nível de perda de pacotes para o caminho:

   a. Ative o botão **Balanceamento adaptativo**.

   b. No campo **Índice mínimo de perda (%)**, especifique a porcentagem mínima de perda de pacotes no caminho na qual o balanceamento adaptativo começa para ajustar o peso. Intervalo de valores: 0,01 a 100.

   c. No campo **Índice máximo de perda (%)**, especifique a porcentagem máxima de perda de pacotes na qual o caminho é excluído do balanceamento de carga.

   d. Na lista suspensa **Velocidade de convergência**, selecione a taxa de convergência dos pesos adaptativos para os valores calculados:

      - **Rápido**: 1
      - **Rápido**: 0,75
      - **Rápido**: 0,5

9. Na lista suspensa **Modo de aprendizado MAC**, selecione a ação que deseja aplicar a uma série de quadros quando o primeiro for enviado ao controlador para saber o endereço MAC de origem:

   - **Aprender e inundar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros será enviada a todas as interfaces de serviço adicionadas ao serviço M2M, exceto à interface de serviço na qual a série de quadros chegou originalmente. Essa é a configuração padrão.
   - **Aprender e descartar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros é descartada.

   Se o endereço MAC de destino estiver presente na tabela MAC, a série de quadros é enviada para a interface de serviço de destino.

10. No campo **Idade do MAC (s)**, insira o tempo (em segundos) durante o qual as entradas são mantidas na tabela MAC do controlador. Intervalo de valores: 10 a 65.535. O valor padrão é `300`.

11. Na lista suspensa **Sobrecarga da tabela MAC**, selecione a política de processamento de novos endereços MAC quando a tabela MAC do controlador está cheia:

    - **Inundação** significa que o tráfego com endereços MAC de destino que não foram aprendidos é transmitido como tráfego BUM (broadcast, unknown-unicast e multicast). Essa é a configuração padrão.
    - **Descartar** significa que o tráfego com endereços MAC de destino que não foram aprendidos é descartado.

12. No campo **Tamanho da tabela MAC**, insira o número máximo de entradas na tabela MAC no controlador. Intervalo de valores: 0 a 65.535. `0` significa que o número de registros na tabela MAC do controlador não é limitado. O valor padrão é `100`.

13. Se necessário, no campo **Descrição**, insira uma breve descrição do serviço M2M.

14. Clique em **Next** para prosseguir para o próximo grupo de configurações.

15. Adicione a interface de serviço ao serviço M2M:

    a. Clique em **+ Adicionar**.

    As configurações da interface de serviço são exibidas.

    b. Nas listas suspensas **Switch** e **Interface de serviço** à direita, selecione o dispositivo CPE e a interface de serviço criada que deseja adicionar ao serviço M2M.

    c. Na lista suspensa **QoS**, selecione a regra de qualidade de serviço criada para a interface de serviço.

    d. Na lista suspensa **Filtro de entrada**, selecione o filtro de tráfego criado para a interface de serviço.

    e. Para adicionar uma interface de serviço de backup através da qual o tráfego deve ser enviado quando a interface de serviço principal falhar, nas listas suspensas **Switch de backup** e **Interface de serviço de backup**, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como interface de serviço de backup.

    Se a interface de serviço principal voltar a ficar on-line, o serviço M2M continua a usar a interface de serviço de backup.

    A interface de serviço é adicionada e exibida na parte inferior da janela. É possível adicionar várias interfaces de serviço ou excluir interfaces de serviço. Para excluir uma interface de serviço, clique no ícone de exclusão ✕ ao lado dela.

16. Clique em **Next** para prosseguir para o próximo grupo de configurações.

17. Para adicionar várias interfaces de rede a um serviço M2M ao mesmo tempo, adicione um grupo de portas OpenFlow. Para isso, execute as seguintes ações:

    a. Clique em **+ Adicionar**.

    As configurações do grupo de portas OpenFlow são exibidas.

    b. Na lista suspensa **Grupo**, selecione o grupo de portas OpenFlow criado que deseja adicionar ao serviço M2M. Ao salvar as configurações do serviço M2M, interfaces de serviço são criadas automaticamente e mapeadas para portas OpenFlow no grupo de portas OpenFlow; em seguida, essas interfaces de serviço são adicionadas automaticamente ao serviço M2M.

    c. Na lista suspensa **QoS**, selecione a regra de qualidade de serviço criada para interfaces de serviço criadas automaticamente e mapeadas para portas OpenFlow.

    d. No campo **ID da VLAN**, insira o valor da tag de VLAN externa para interfaces de serviço criadas automaticamente e mapeadas para portas OpenFlow. As interfaces de serviço do tipo classificação de VLAN só podem ser criadas automaticamente. A mesma tag de VLAN externa é atribuída a cada interface de serviço.

    O grupo OpenFlow é adicionado e exibido na parte inferior da janela. É possível adicionar vários grupos de portas OpenFlow ou excluir grupos de portas OpenFlow. Para excluir um grupo de portas OpenFlow, clique no ícone de exclusão ✕ ao lado dele.

18. Clique em **Criar**.

O serviço M2M é criado e exibido na tabela.

Visualizar as estatísticas de um serviço M2M

Para visualizar as estatísticas de um serviço M2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços M2M**.

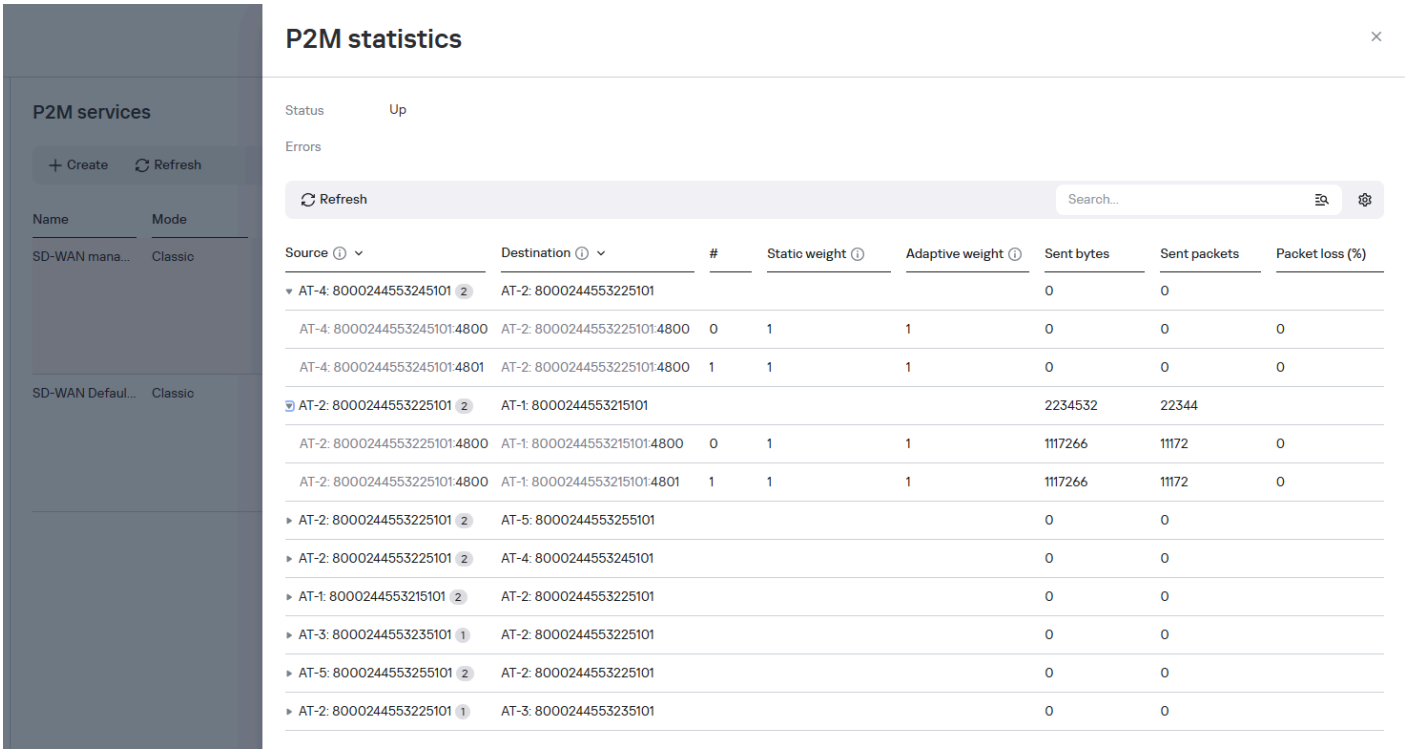
   Uma tabela de serviços M2M é exibida.

4. Clique em **Gerenciamento** → **Estatísticas** ao lado do serviço M2M cujas estatísticas deseja visualizar.

Isso abre uma janela com estatísticas do serviço M2M.

Na parte superior da janela de estatísticas, o campo **Status** exibe o status operacional do serviço. O campo **Erros** exibe possíveis erros que podem ocorrer para o serviço.

As estatísticas de segmentos, caminhos e links do serviço são exibidas hierarquicamente em uma tabela. As linhas da tabela são agrupadas por segmento. As linhas dentro de cada grupo contêm estatísticas dos caminhos incluídos no segmento correspondente. Para expandir um grupo, clique no triângulo (▸). Para serviços sem limites definidos, as linhas exibem todos os caminhos com balanceamento de carga ativado no segmento. Para serviços com limites, as linhas exibem os caminhos de Auto-TE que atendem aos limites.



Exibição de estatísticas usando um serviço P2M como exemplo

As informações estatísticas detalhadas sobre segmentos e caminhos são exibidas nas seguintes colunas da tabela:

Origem: para linhas agregadas, o host de origem do segmento; para linhas em grupos expansíveis, o host de origem do caminho no segmento.

Destino: para linhas agregadas, o host de destino do segmento; para linhas em grupos expansíveis, o host de destino do caminho no segmento.

é o número sequencial do caminho. Quanto menor o número do caminho, há mais tempo ele foi criado. Esse valor é exibido apenas nas linhas em grupos expansíveis.

Peso estático é o peso do caminho estático com base no custo. Esse valor é exibido apenas para linhas em grupos expansíveis.

Peso adaptativo é o peso dinâmico do caminho com base na análise da perda de pacotes nesse caminho. Esse valor é exibido apenas para linhas em grupos expansíveis. Se o balanceamento adaptativo não for usado, essa coluna não é exibida.

Bytes enviados: para linhas agregadas, o valor da janela de estatísticas do serviço atual; para linhas em grupos expansíveis, o número de bytes enviados ao bucket do grupo OF.

Pacotes enviados: para linhas agregadas, o valor da janela de estatísticas do serviço atual; para linhas em grupos expansíveis, o número de pacotes enviados ao bucket do grupo OF.

Perda de pacotes (%) é a porcentagem de perda de pacotes em um determinado caminho (a razão entre o número de pacotes perdidos e o número total de pacotes enviados). Esse valor é exibido apenas nas linhas em grupos expansíveis.

Visualizar a tabela MAC de um serviço M2M

Para visualizar a tabela MAC de um serviço M2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços M2M**.

   Uma tabela de serviços M2M é exibida.

4. Clique em **Gerenciamento** → **Tabela MAC** ao lado do serviço M2M cujas estatísticas deseja visualizar.

Isso abre uma janela com a tabela MAC do serviço M2M. As informações sobre os endereços MAC são exibidas nas seguintes colunas da tabela:

- **MAC** é o endereço MAC.
- **Nome do host** é o DPID do switch onde está localizado o endereço MAC.
- **Porta** é o número da porta onde está localizado o endereço MAC.
- **VLAN** é o segmento da VLAN onde está localizado o endereço MAC.
- **Idade (s)** é o tempo em segundos durante o qual o endereço MAC esteve presente na tabela de endereços MAC.

5. Para encontrar um endereço MAC específico, insira-o no campo e clique em **Encontrar pelo MAC**.
6. Para limpar a tabela MAC, clique em **Limpar**.

Visualizar e configurar a exibição de uma topologia de serviço M2M

Para visualizar e configurar a exibição de uma topologia de serviço M2M

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços M2M**.

   Uma tabela de serviços M2M é exibida.

4. Clique em **Gerenciamento** → **Topologia de serviço** ao lado do serviço M2M cuja topologia deseja visualizar.

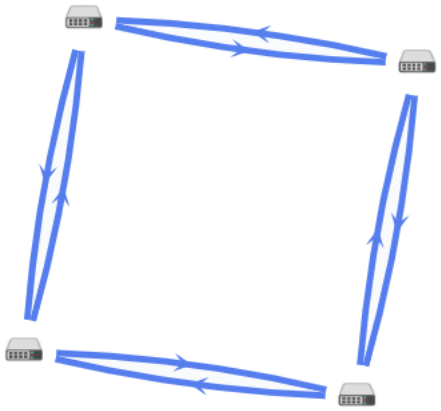
   Isso abre uma janela com a topologia do serviço M2M.

5. Caso seja necessário mover dispositivos CPE, execute uma das seguintes ações:

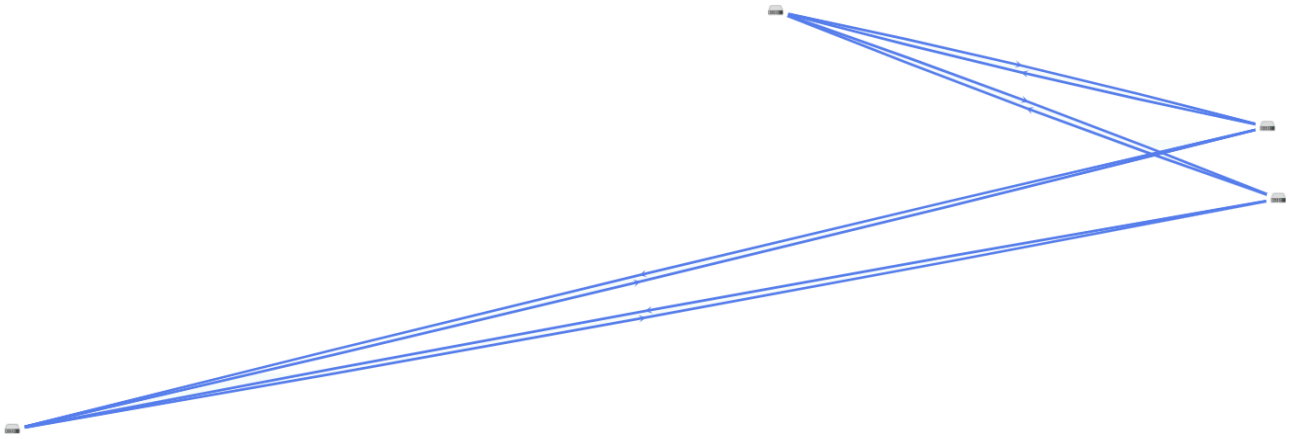
- Para alterar manualmente a posição dos dispositivos CPE, clique em **Manual** e ajuste a posição dos dispositivos.

- Para organizar dispositivos CPE automaticamente, clique em **Automaticamente** e selecione um dos seguintes valores na lista suspensa exibida:

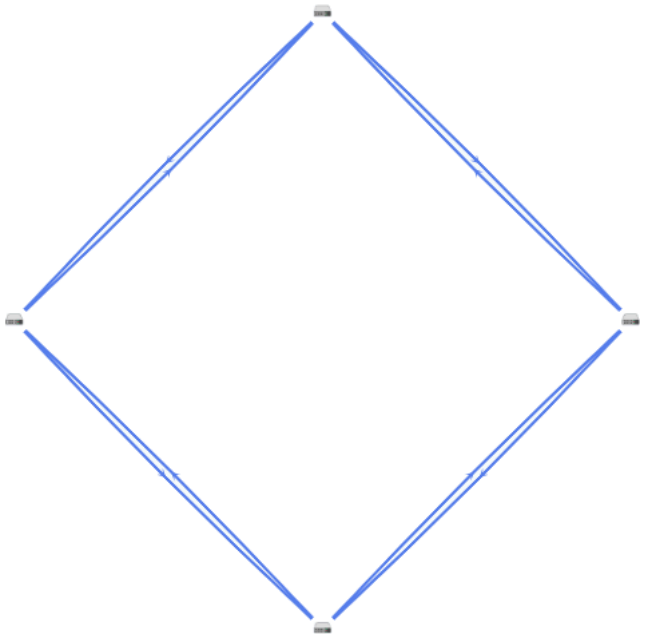
  - **Simulação física** — Os dispositivos CPE são organizados aproximadamente de acordo com sua localização real em relação uns aos outros, por exemplo:



  - **Aleatório** — A organização dos dispositivos CPE é aleatória, por exemplo:

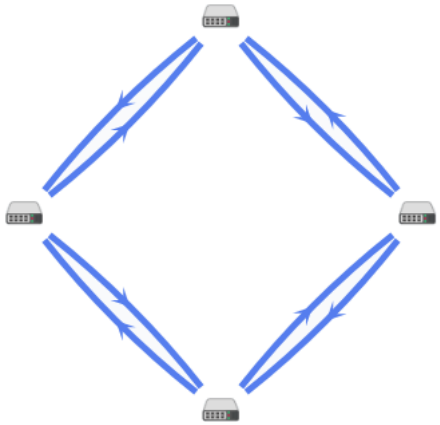


  - **Círculo** — Os dispositivos CPE são organizados de acordo com uma topologia em anel, por exemplo:



- **Em largura** — Os dispositivos CPE são organizados horizontalmente, por exemplo:

- **Concêntrico** — Os dispositivos CPE são organizados de forma concêntrica, por exemplo:



- **Grade** — Os dispositivos CPE são organizados de acordo com uma topologia de grade, por exemplo:

6. Para exibir informações sobre dispositivos CPE, marque as seguintes caixas de seleção:

   - **Nome** exibe os nomes dos dispositivos CPE.
   - **Endereço IP** exibe os endereços IP dos dispositivos CPE.

   Essas caixas de seleção são desmarcadas por padrão.

7. Para exibir um segmento entre dois dispositivos CPE:

   a. Marque a caixa de seleção **Segmentos**. Esta caixa de seleção está desmarcada por padrão.

   b. Nas listas suspensas exibidas, selecione os dispositivos CPE de origem e destino do segmento.

   O segmento entre os dispositivos CPE é exibido.

Editar um serviço M2M

Para editar um serviço M2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços M2M**.

   Uma tabela de serviços M2M é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do serviço M2M que deseja editar.

5. Na janela aberta, se necessário, edite as configurações do serviço M2M. Para obter uma descrição das configurações, consulte as instruções para criar um serviço M2M.

6. Clique em **Salvar**.

O serviço M2M é modificado e atualizado na tabela.

Reiniciar um serviço M2M

É possível reiniciar um serviço M2M para restaurá-lo em caso de mau funcionamento. Ao reiniciar um serviço M2M, o controlador exclui e recria automaticamente as regras associadas ao serviço M2M nas tabelas OpenFlow dos dispositivos CPE. Isso afeta os dispositivos CPE cujas interfaces de serviço são adicionadas ao serviço M2M.

Para reiniciar um serviço M2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços M2M**.

   Uma tabela de serviços M2M é exibida.

4. Clique em **Gerenciamento** → **Reaprovisionamento** ao lado do serviço M2M que deseja reprovisionar.

5. Na janela de confirmação, clique em **Confirmar**.

O serviço M2M é reiniciado.

Excluir um serviço M2M

Os serviços M2M excluídos não podem ser restaurados.

Para excluir um serviço M2M:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços M2M**.

   Uma tabela de serviços M2M é exibida.

4. Clique em **Gerenciamento** → **Excluir** ao lado do serviço M2M que deseja excluir.

5. Para excluir as interfaces de serviço adicionadas ao serviço M2M, marque a caixa de seleção **Excluir interfaces de serviço associadas** na janela de confirmação. Esta caixa de seleção está desmarcada por padrão.

6. Clique em **Excluir**.

O serviço M2M é excluído e não é mais exibido na tabela.

Gerenciar serviços de transporte multicast IP

Para visualizar a tabela de serviços multicast IP, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Serviços multicast IP**. As informações sobre os serviços multicast IP são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do serviço multicast IP.
- **Interface de serviço de origem** contém informações sobre a interface de serviço de origem do serviço multicast IP:
  - Nome e DPID do dispositivo CPE no qual a interface de serviço foi criada
  - O número da porta OpenFlow para a qual a interface de serviço é mapeada
- **Interface de serviço de backup** contém informações sobre a interface de serviço de origem de backup do serviço multicast IP:
  - Nome e DPID do dispositivo CPE no qual a interface de serviço foi criada
  - O número da porta OpenFlow para a qual a interface de serviço é mapeada
- **IP do consultor** é o endereço IP da interface de serviço de origem do serviço multicast IP.
- **Interfaces de serviço para o consumidor** contém informações sobre as interfaces de serviço de destino do serviço multicast IP:
  - Nomes e DPIDs dos dispositivos CPE nos quais as interfaces de serviço foram criadas
  - Números de portas OpenFlow para as quais as interfaces de serviço são mapeadas
- **Grupos** contém informações sobre grupos multicast adicionados ao serviço multicast IP:
  - Endereços IP de grupos multicast
  - Comprimentos de prefixo de grupos multicast
  - Largura de banda garantida para grupos multicast

- **Status** é o status do serviço multicast IP:
  - **Para cima**
  - **Para baixo**
- **Erros** são erros ocorridos enquanto o serviço multicast IP estava em execução.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um serviço multicast IP

Para criar um serviço multicast IP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços multicast IP**.

   Uma tabela de serviços multicast IP é exibida.

4. Na parte superior da página, clique em **+ Serviço multicast IP**.

5. Na janela aberta, no campo **Nome**, insira o nome do serviço multicast IP.

6. Nas listas suspensas **Switch de origem** e **Interface de serviço de origem**, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como interface de serviço de origem do serviço multicast IP.

7. Para exibir interfaces de serviço adicionadas aos serviços de transporte na lista suspensa **Interface de serviço de origem**, marque a caixa de seleção **Mostrar interfaces usadas**. Esta caixa de seleção está desmarcada por padrão.

8. No campo **IP do consultor**, insira o endereço IP da interface de serviço de origem do serviço multicast IP.

9. Para adicionar uma interface de serviço reserva da fonte de serviço multicast IP através da qual o tráfego é transmitido se a interface de serviço principal falhar:

   a. Marque a caixa de seleção **Usar interface de backup**. Esta caixa de seleção está desmarcada por padrão.

   b. Nas listas suspensas **Switch de backup** e**Interface de serviço de backup**, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como reserva.

   c. Para exibir interfaces de serviço adicionadas aos serviços de transporte, na lista suspensa **Interface de serviço de backup**, marque a caixa de seleção **Mostrar interfaces usadas**. Esta caixa de seleção está desmarcada por padrão.

d. Para que o serviço multicast IP volte a usar a interface de serviço de origem principal quando ela for ativada novamente, marque a caixa de seleção **Retorno automático de recuperação**. Esta caixa de seleção está desmarcada por padrão.

e. Para que a árvore de distribuição de tráfego multicast seja criada na interface do serviço reserva, marque a caixa de seleção **Árvore multicast de backup**. Enquanto a interface de serviço principal estiver ativa, os pacotes de tráfego na interface de serviço reserva serão descartados. Esta caixa de seleção é selecionada por padrão.

10. Marque a caixa de seleção **Proxy IGMP** para usar um servidor proxy IGMP. Isso permite manter a transmissão de tráfego para grupos multicast ativos aos quais pelo menos uma interface de serviço de destino do serviço multicast IP está conectado. Esta caixa de seleção está desmarcada por padrão.

11. Na lista suspensa **QoS**, selecione a regra de qualidade de serviço criada para a interface de serviço da origem do serviço multicast IP.

12. Clique em **Next** para prosseguir para o próximo grupo de configurações.

13. Adicione a interface de serviço de destino ao serviço multicast IP:

    a. Nas listas suspensas **Switch do consumidor** e **Interface de serviço para o consumidor**, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como interface de serviço de destino do serviço multicast IP.

    b. Para exibir interfaces de serviço adicionadas aos serviços de transporte na lista suspensa **Interface de serviço para o consumidor**, marque a caixa de seleção **Mostrar interfaces usadas**. Esta caixa de seleção está desmarcada por padrão.

    c. Clique em **+ Adicionar**.

    A interface de serviço é adicionada e exibida na parte inferior da janela. É possível adicionar várias interfaces de serviço ou excluir interfaces de serviço. Para excluir uma interface de serviço, clique em **Excluir** ao lado dela.

14. Clique em **Next** para prosseguir para o próximo grupo de configurações.

15. Adicione o grupo multicast ao serviço multicast IP:

    a. No campo **Endereço IP**, insira o endereço IP do grupo multicast. Intervalo de valores: 224.0.0.0 a 239.255.255.255.

    b. Na lista suspensa **Máscara**, selecione o comprimento do prefixo do grupo multicast. Intervalo de valores: 24 a 32.

    c. Na lista suspensa **GBR**, selecione a taxa de bits garantida (GBR) para o grupo multicast.

    d. Clique em **+ Adicionar**.

    O grupo multicast é adicionado e exibido na parte inferior da janela. É possível adicionar vários grupos multicast ou excluir grupos multicast. Para excluir um grupo multicast, clique em **Excluir** ao lado dele.

16. Clique em **Criar**.

O serviço multicast IP é criado e exibido na tabela.

Visualizar as estatísticas de um serviço multicast IP

Para visualizar as estatísticas de um serviço multicast IP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços multicast IP**.

   Uma tabela de serviços multicast IP é exibida.

4. Clique em **Gerenciamento** → **Estatísticas** ao lado do serviço multicast IP cujas estatísticas deseja visualizar.

Isso abre uma janela com estatísticas do serviço multicast IP.

Editar um serviço multicast IP

Para editar um serviço multicast IP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços multicast IP**.

   Uma tabela de serviços multicast IP é exibida.

4. Clique em **Gerenciamento** → **Editar interfaces de origem**, **Editar interfaces do consumidor** ou **Editar grupos multicast** ao lado do serviço multicast IP que deseja editar.

5. Na janela aberta, se necessário, edite as configurações do serviço multicast IP. Para obter uma descrição das configurações, consulte as instruções para criar um serviço multicast IP.

6. Clique em **Salvar**.

O serviço multicast IP é modificado e atualizado na tabela.

Excluir um serviço multicast IP

Os serviços multicast IP excluídos não podem ser restaurados.

Para excluir um serviço multicast IP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços multicast IP**.

   Uma tabela de serviços multicast IP é exibida.

4. Clique em **Gerenciamento** → **Excluir** ao lado do serviço multicast IP que deseja excluir.

5. Para excluir as interfaces de serviço adicionadas ao serviço multicast IP, marque a caixa de seleção **Excluir interfaces de serviço associadas** na janela de confirmação. Esta caixa de seleção está desmarcada por padrão.

6. Clique em **Excluir**.

O serviço multicast IP é excluído e não é mais exibido na tabela.

Gerenciar serviços de transporte VPN L3

Para visualizar a tabela de serviços de VPN L3, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Serviços de L3 VPN**. As informações sobre os serviços de VPN L3 são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do serviço de VPN L3.
- **Tipo** é o tipo de topologia do serviço de VPN L3.
- **Inter-spoke por hub** indica se a comunicação entre sites spoke por meio do site hub é possível:
  - **Sim**.
  - **Não**.

- **Endpoints** são as informações sobre as interfaces L3 adicionadas ao serviço de VPN L3:
  - Se as interfaces L3 estiverem mapeadas para serviços M2M, os nomes dos serviços M2M são exibidos.
  - Se as interfaces L3 estiverem mapeadas para interfaces de serviço, as seguintes informações são exibidas:
    - Nomes e DPIDs dos dispositivos CPE nos quais as interfaces de serviço foram criadas
    - Números de portas OpenFlow para as quais as interfaces de serviço são mapeadas
    - Regras de qualidade de serviço especificadas para as interfaces de serviço
    - Filtros de tráfego especificados para as interfaces de serviço
  - Comprimentos dos prefixos da interface L3.
  - Endereços MAC das interfaces L3
  - Tempo em segundos durante o qual as entradas são mantidas na tabela ARP do controlador
- **Rotas** são as informações sobre as rotas estáticas adicionadas ao serviço de VPN L3:
  - Prefixos IPv4 de destino de rotas estáticas
  - Endereços IPv4 de gateway para rotear pacotes de tráfego para prefixos IPv4 de destino de rotas estáticas
  - Interfaces L3 das quais os prefixos IPv4 de destino de rotas estáticas estão atrás
  - Métricas das rotas estáticas
- **Status** é o status do serviço de VPN L3:
  - **Para cima**
  - **Para baixo**
- **Erros** são erros ocorridos enquanto o serviço de VPN L3 estava em execução.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um serviço de VPN L3

Para criar um serviço de VPN L3:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços de L3 VPN**.

   Uma tabela de serviços de VPN L3 é exibida.

4. Na parte superior da página, clique em **+ Serviço de L3 VPN**.

5. Na janela aberta, no campo **Nome**, insira o nome do serviço de VPN L3.

6. Na lista suspensa **Restrição**, selecione a restrição de Manual-TE criada ou a restrição de limite que deseja adicionar ao serviço de VPN L3.

7. Na lista suspensa **Modo de balanceamento**, selecione o modo de balanceamento para balancear o tráfego em todos os links:

   - **Por fluxo** significa que os fluxos de tráfego (5-Tuple) são distribuídos entre os links de acordo com o custo do link. Essa é a configuração padrão.
   - **Por pacote** significa que os pacotes de tráfego são distribuídos entre os links de acordo com o custo do link.
   - **Difusão** significa que os pacotes de tráfego são duplicados e transmitidos simultaneamente por todos os links para evitar perdas.

   É possível especificar o custo do link manualmente.

8. É possível configurar o modo de balanceamento adaptativo caso deseje que o peso do caminho seja ajustado dinamicamente dependendo do nível de perda de pacotes para o caminho:

   a. Ative o botão **Balanceamento adaptativo**.

   b. No campo **Índice mínimo de perda (%)**, especifique a porcentagem mínima de perda de pacotes no caminho na qual o balanceamento adaptativo começa para ajustar o peso. Intervalo de valores: 0,01 a 100.

   c. No campo **Índice máximo de perda (%)**, especifique a porcentagem máxima de perda de pacotes na qual o caminho é excluído do balanceamento de carga.

   d. Na lista suspensa **Velocidade de convergência**, selecione a taxa de convergência dos pesos adaptativos para os valores calculados:

      - **Rápido**: 1
      - **Rápido**: 0,75
      - **Rápido**: 0,5

9. Clique em **Next** para prosseguir para o próximo grupo de configurações.

10. Adicione a interface L3 ao serviço de VPN L3:

    a. Na lista suspensa **Modo**, selecione o tipo da interface L3:

       - **Serviço M2M** significa que a interface L3 é mapeada para um serviço M2M.
       - **Interface de serviço** significa que a interface L3 é mapeada para uma interface de serviço.

b. Caso tenha selecionado **Serviço M2M** na lista suspensa **Modo**, na lista suspensa **Serviço M2M**, selecione o serviço M2M criado mapeado para a interface L3.

c. Caso tenha selecionado **Interface de serviço** na lista suspensa **Modo**, configure a interface de serviço:

1. Nas listas suspensas **Switch** e**Interface de serviço**, selecione o dispositivo CPE e a interface de serviço criada para a qual a interface L3 é mapeada.

2. Na lista suspensa **QoS**, selecione a regra de qualidade de serviço criada para a interface L3.

3. Na lista suspensa **Filtro de entrada**, selecione o filtro de tráfego criado para a interface L3.

4. Para exibir interfaces de serviço adicionadas aos serviços de transporte na lista suspensa **Interface de serviço**, marque a caixa de seleção **Mostrar interfaces usadas**. Esta caixa de seleção está desmarcada por padrão.

d. No campo **Endereço IP**, insira o endereço IP da interface L3.

e. No campo **Comprimento do prefixo**, insira o comprimento do prefixo da interface L3. Intervalo de valores: 0 a 32.

f. No campo **Endereço MAC**, insira o endereço MAC da interface L3. Para gerar um endereço MAC, clique em **Gerar**.

g. No campo **Idade do ARP (s)**, insira o tempo, em segundos, durante o qual as entradas são mantidas na tabela ARP do serviço de VPN L3. Intervalo de valores: 1 a 65.535. O valor padrão é `200`.

h. Clique em **+ Adicionar**.

A interface L3 é adicionada e exibida na parte inferior da janela. É possível adicionar várias interfaces L3 ou excluir interfaces L3. Para excluir uma interface L3, clique em **Excluir** ao lado dela.

11. Clique em **Next** para prosseguir para o próximo grupo de configurações.

12. Para adicionar uma rota estática ao serviço de VPN L3:

a. No campo **Endereço IP**, insira o endereço IPv4 de destino da rota estática.

b. No campo **Comprimento do prefixo**, insira o comprimento do prefixo IPv4 da rota estática. Intervalo de valores: 0 a 32.

c. Na lista suspensa **SVI**, selecione a interface L3 adicionada seguida pelo prefixo IPv4 do destino da rota estática. Você adicionou uma interface L3 na etapa 9 destas instruções.

d. No campo **Gateway**, insira o endereço IPv4 do gateway para rotear pacotes de tráfego para o prefixo IPv4 do destino da rota estática.

e. No campo **Métrica**, insira uma métrica para a rota estática. O valor padrão é `0`.

f. Clique em **+ Adicionar**.

A rota estática é adicionada e exibida na parte inferior da janela. É possível adicionar várias rotas estáticas ou excluir rotas estáticas. Para excluir uma rota estática, clique em **Excluir** ao lado dela.

13. Clique em **Criar**.

O serviço de VPN L3 é criado e exibido na tabela.

Gerenciar a tabela ARP de um serviço de VPN L3

Para visualizar a tabela ARP do serviço de VPN L3, vá para a seção **Infraestrutura**, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador, vá para a seção **Serviços de L3 VPN** e clique em **Gerenciamento** → **Tabela de ARP** ao lado do serviço de VPN L3. As informações sobre os registros são exibidas nas seguintes colunas da tabela:

- **Endereço IP** é o endereço IP da interface de serviço.
- **MAC** é o endereço MAC da interface de serviço.
- **Interface de serviço** são as informações sobre a interface de serviço:
  - Nome e DPID do dispositivo CPE no qual a interface de serviço foi criada
  - O número da porta OpenFlow para a qual a interface de serviço é mapeada
- **Tempo limite máximo (s)** é o tempo em segundos decorrido desde que o registro foi criado.

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um registro estático na tabela ARP de um serviço de VPN L3

Para criar um registro estático na tabela ARP de um serviço de VPN L3:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços de L3 VPN**.

   Uma tabela de serviços de VPN L3 é exibida.

4. Clique em **Gerenciamento** → **Tabela de ARP** ao lado do serviço de VPN L3 em cuja tabela ARP deseja criar um registro estático.

   A página com a tabela ARP do serviço de VPN L3 é exibida.

5. Na parte superior da página, clique em **+ Registro de ARP estático**.

6. Na janela aberta, nas listas suspensas **Switch** e **Interface de serviço**, selecione o dispositivo CPE e a interface de serviço criada para a qual deseja especificar um endereço IP e um endereço MAC.

7. No campo **Endereço IP**, insira o endereço IP da interface de serviço.

8. No campo **MAC**, insira o endereço MAC da interface de serviço.

9. Clique em **Criar**.

O registro estático é criado e exibido na tabela ARP do serviço de VPN L3.

Editar um registro estático na tabela ARP de um serviço de VPN L3

Para editar um registro estático na tabela ARP de um serviço de VPN L3:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços de L3 VPN**.

   Uma tabela de serviços de VPN L3 é exibida.

4. Clique em **Gerenciamento** → **Tabela de ARP** ao lado do serviço de VPN L3 em cuja tabela ARP deseja editar um registro estático.

   A página com a tabela ARP do serviço de VPN L3 é exibida.

5. Clique em **Gerenciamento** → **Editar** ao lado do registro estático que deseja editar.

6. Na janela aberta, se necessário, edite o endereço IP e/ou o endereço MAC da interface de serviço.

7. Clique em **Salvar**.

O registro estático é modificado e atualizado na tabela.

Excluir um registro estático na tabela ARP de um serviço de VPN L3

Os registros estáticos excluídos na tabela ARP de um serviço de VPN L3 não podem ser restaurados.

Para excluir um registro estático na tabela ARP de um serviço de VPN L3:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços de L3 VPN**.

   Uma tabela de serviços de VPN L3 é exibida.

4. Clique em **Gerenciamento** → **Tabela de ARP** ao lado do serviço de VPN L3 em cuja tabela ARP deseja excluir um registro estático.

   A página com a tabela ARP do serviço de VPN L3 é exibida.

5. Clique em **Gerenciamento** → **Excluir** ao lado do registro estático que deseja excluir.

6. Na janela de confirmação, clique em **Excluir**.

O registro estático é excluído e não é mais exibido na tabela.

Visualizar a tabela de roteamento e encaminhamento de um serviço de VPN L3

Para visualizar a tabela de roteamento e encaminhamento de um serviço de VPN L3:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços de L3 VPN**.

   Uma tabela de serviços de VPN L3 é exibida.

4. Clique em **Gerenciamento** → **Tabela de roteamento** ao lado do serviço de VPN L3 cuja tabela de roteamento deseja visualizar.

Isso abre uma janela com a tabela de roteamento e encaminhamento do serviço de VPN L3.

Editar um serviço de VPN L3

Para editar um serviço de VPN L3:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços de L3 VPN**.

   Uma tabela de serviços de VPN L3 é exibida.

4. Clique em **Gerenciamento** → **Editar** ao lado do serviço de VPN L3 que deseja editar.

5. Na janela aberta, se necessário, edite as configurações do serviço de VPN L3. Para obter uma descrição das configurações, consulte as instruções para criar um serviço de VPN L3.

6. Clique em **Salvar**.

O serviço de VPN L3 é modificado e atualizado na tabela.

Reiniciar um serviço de VPN L3

É possível reiniciar um serviço de VPN L3 para restaurá-lo em caso de mau funcionamento. Ao reiniciar um serviço de VPN L3, o controlador exclui e recria automaticamente as regras associadas ao serviço de VPN L3 nas tabelas OpenFlow dos dispositivos CPE. Isso afeta os dispositivos CPE cujas interfaces de serviço são adicionadas ao serviço de VPN L3.

Para reiniciar um serviço de VPN L3:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços de L3 VPN**.

   Uma tabela de serviços de VPN L3 é exibida.

4. Clique em **Gerenciamento** → **Reaprovisionamento** ao lado do serviço de VPN L3 que deseja reprovisionar.

5. Na janela de confirmação, clique em **Confirmar**.

O serviço de VPN L3 é reiniciado.

Excluir um serviço de VPN L3

Os serviços de VPN L3 excluídos não podem ser restaurados.

Para excluir um serviço de VPN L3:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços de L3 VPN**.

   Uma tabela de serviços de VPN L3 é exibida.

4. Clique em **Gerenciamento** → **Excluir** ao lado do serviço de VPN L3 que deseja excluir.

5. Para excluir as interfaces de serviço adicionadas ao serviço de VPN L3, marque a caixa de seleção **Excluir interfaces de serviço associadas** na janela de confirmação. Esta caixa de seleção está desmarcada por padrão.

6. Clique em **Excluir**.

O serviço de VPN L3 é excluído e não é mais exibido na tabela.

Gerenciar serviços de transporte em um modelo de instância SD-WAN

Para visualizar a tabela de serviços P2M e M2M em um modelo de instância SD-WAN, vá para a seção **SD-WAN** → **Modelos de instância SD-WAN**, clique no modelo de instância SD-WAN e selecione a guia **Serviços de transporte**. As informações sobre os serviços P2M e M2M são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do serviço P2M ou M2M.
- **Tipo** é o tipo de serviço de transporte:
  - **P2M**
  - **M2M**
- **Serviço de transporte de gerenciamento** indica se o serviço P2M ou M2M é um serviço de gerenciamento:
  - **Sim**.
  - **Não**.
- **Modo** indica se uma DFI (Interface de encaminhamento padrão) é usada no serviço P2M para o qual o tráfego unicast desconhecido é enviado:
  - **Clássico** caso não deseje usar uma DFI. Essa é a configuração padrão.
  - **DFI com FIB na raiz e folhas** para usar uma DFI na interface de serviço com a função raiz.
  - **DFI com FIB na folha** para usar uma DFI na interface de serviço com a função raiz. As interfaces de serviço com a função folha devem ser criadas no mesmo dispositivo CPE. As interfaces de serviço de backup com a função folha devem ser criadas no mesmo dispositivo CPE, que deve ser diferente do dispositivo CPE no qual as interfaces de serviço principais foram criadas.

  O valor dessa coluna só é exibido se o valor na coluna **Tipo** for **P2M**.

- **Idade do MAC (s)** é o tempo, em segundos, durante o qual as entradas são mantidas na tabela MAC do controlador.

- **Modo de aprendizado MAC** é a ação aplicada a uma série de quadros quando o primeiro quadro é enviado ao controlador para aprender o endereço MAC de origem:

  - **Aprender e inundar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros será enviada a todas as interfaces de serviço adicionadas ao serviço M2M, exceto à interface de serviço na qual a série de quadros chegou originalmente.

  - **Aprender e descartar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros é descartada.

  Se o endereço MAC de destino estiver presente na tabela MAC, a série de quadros é enviada para a interface de serviço de destino.

- **Tamanho da tabela MAC** é o número máximo de entradas na tabela MAC no controlador.

- **Sobrecarga da tabela MAC** é a política de processamento de novos endereços MAC quando a tabela MAC do controlador está cheia:

  - **Inundação** significa que o tráfego com endereços MAC de destino que não foram aprendidos é transmitido como tráfego BUM (broadcast, unknown-unicast e multicast). Essa é a configuração padrão.

  - **Descartar** significa que o tráfego com endereços MAC de destino que não foram aprendidos é descartado.

- **Ações** contém as ações que podem ser executadas com o serviço de transporte.

Para visualizar uma lista de serviços de VPN L3, selecione a guia **Serviços L3**.

Criar um serviço P2M ou M2M em um modelo de instância SD-WAN

Para criar um serviço P2M ou M2M em um modelo de instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN no qual deseja criar um serviço P2M ou M2M.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Selecione a guia **Serviços de transporte**.

   A guia **Serviços X2M** com a tabela de serviços P2M e M2M é selecionada por padrão.

4. Clique em **+Serviço de transporte**.

5. Na janela aberta, no campo **Nome**, insira o nome do serviço P2M ou M2M.

6. Na lista suspensa **Tipo**, selecione o tipo do serviço de transporte:

   - **P2M** Caso tenha selecionado essa opção na lista suspensa **Modo**, selecione se o serviço P2M usa uma DFI (Interface de encaminhamento padrão), para a qual o tráfego unicast desconhecido é enviado:

     - **Clássico** caso não deseje usar uma DFI. Essa é a configuração padrão.

     - **DFI com FIB na raiz e folhas** para usar uma DFI na interface de serviço com a função raiz.

     - **DFI com FIB na folha** para usar uma DFI na interface de serviço com a função raiz. As interfaces de serviço com a função folha devem ser criadas no mesmo dispositivo CPE. As interfaces de serviço de backup com a função folha devem ser criadas no mesmo dispositivo CPE, que deve ser diferente do dispositivo CPE no qual as interfaces de serviço principais foram criadas.

   - **M2M**

7. Para tornar um serviço P2M ou M2M o serviço de gerenciamento, marque a caixa de seleção **Serviço de transporte de gerenciamento**. Esta caixa de seleção está desmarcada por padrão. Apenas um serviço de transporte pode ser o serviço de gerenciamento.

8. Na lista suspensa **Modo de aprendizado MAC**, selecione a ação que deseja aplicar a uma série de quadros quando o primeiro for enviado ao controlador para saber o endereço MAC de origem:

   - **Aprender e inundar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros será enviada para todas as interfaces de serviço adicionadas ao serviço P2M, exceto para a interface de serviço na qual a série de quadros chegou originalmente. Essa é a configuração padrão.

   - **Aprender e descartar** significa que o controlador lembra do endereço MAC da origem e verifica a presença do endereço MAC de destino na tabela MAC. Se o endereço MAC de destino não estiver na tabela MAC, a série de quadros é descartada.

   Se o endereço MAC de destino estiver presente na tabela MAC, a série de quadros é enviada para a interface de serviço de destino.

9. No campo **Tamanho da tabela MAC**, insira o número máximo de entradas na tabela MAC no controlador. Intervalo de valores: 0 a 65.535. `0` significa que o número de registros na tabela MAC do controlador não é limitado. O valor padrão é `100`.

10. No campo **Idade do MAC (s)**, insira o tempo (em segundos) durante o qual as entradas são mantidas na tabela MAC do controlador. Intervalo de valores: 10 a 65.535. O valor padrão é `300`.

11. Na lista suspensa **Sobrecarga da tabela MAC**, selecione a política de processamento de novos endereços MAC quando a tabela MAC do controlador está cheia:

    - **Inundação** significa que o tráfego com endereços MAC de destino que não foram aprendidos é transmitido como tráfego BUM (broadcast, unknown-unicast e multicast). Essa é a configuração padrão.

    - **Descartar** significa que o tráfego com endereços MAC de destino que não foram aprendidos é descartado.

12. Clique em **Criar**.

    Um serviço P2M ou M2M é criado e exibido na tabela.

13. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Criar um serviço de VPN L3 em um modelo de instância SD-WAN

Para criar um serviço de VPN L3 em um modelo de instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN no qual deseja criar um serviço de VPN L3.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Selecione a guia **Serviços de transporte → Serviços L3**.

   Uma lista de serviços de VPN L3 é exibida.

4. Clique em **+Serviço de transporte**.

5. Na janela aberta, insira o nome do serviço de VPN L3.

6. Clique em **Criar**.

   O serviço de VPN L3 é criado e exibido na tabela.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Editar um serviço de transporte em um modelo de instância SD-WAN

Para editar um serviço de transporte em um modelo de instância SD-WAN:

1. No menu, acesse a seção **SD-WAN → Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN no qual deseja editar um serviço de transporte.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Para editar um serviço P2M ou M2M:

   a. Selecione a guia **Serviços de transporte**.

      A guia **Serviços X2M** com a tabela de serviços P2M e M2M é selecionada por padrão.

   b. Clique em **Editar** ao lado do serviço P2M ou M2M que deseja editar.

   c. Na janela aberta, se necessário, edite as configurações do serviço P2M ou M2M. Para obter uma descrição das configurações, consulte as instruções para criar um serviço P2M ou M2M em um modelo de instância SD-WAN.

4. Para editar um serviço de VPN L3:

   a. Selecione a guia **Serviços de transporte** → **Serviços L3**.

      Uma lista de serviços de VPN L3 é exibida.

   b. Clique em **Editar** ao lado do serviço de VPN L3 que deseja editar.

   c. Na janela aberta, se necessário, edite o nome do serviço de VPN L3.

5. Clique em **Salvar**.

   O serviço de transporte é modificado e atualizado na tabela.

6. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Excluir um serviço de transporte em um modelo de instância SD-WAN

Os serviços de transporte excluídos no modelo de instância SD-WAN não podem ser restaurados.

Para excluir um serviço de transporte em um modelo de instância SD-WAN:

1. No menu, acesse a seção **SD-WAN** → **Modelos de instância SD-WAN**.

   Uma tabela de modelos de instância SD-WAN é exibida.

2. Clique no modelo de instância SD-WAN do qual deseja excluir um serviço de transporte.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher toda a página clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe o nome do modelo de instância SD-WAN.

3. Para excluir um serviço P2M ou M2M:

   a. Selecione a guia **Serviços de transporte**.

      A guia **Serviços X2M** com a tabela de serviços P2M e M2M é selecionada por padrão.

   b. Clique em **Excluir** ao lado do serviço P2M ou M2M que deseja excluir.

   O serviço P2M ou M2M é excluído e não é mais exibido na tabela.

4. Para excluir um serviço de VPN L3:

   a. Selecione a guia **Serviços de transporte** → **Serviços L3**.

      Uma lista de serviços VPN L3 é exibida.

   b. Clique em **Excluir** ao lado do serviço de VPN L3 que deseja excluir.

O serviço VPN L3 é excluído e não é mais exibido na tabela.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de instância SD-WAN.

Gerenciar serviços de transporte em um modelo de CPE

Para visualizar a tabela de serviços de transporte em um modelo de CPE, vá para a seção **SD-WAN → Modelos de CPE** do menu, clique no modelo de CPE e selecione a guia **Serviços de transporte**. As informações sobre os serviços de transporte são exibidas nas seguintes colunas da tabela:

- **Nome** é o nome do serviço de transporte.
- **Nome do QoS** é o nome da regra de qualidade de serviço para a interface de serviço, que é criada automaticamente para conectar o dispositivo CPE ao serviço de transporte.
- **Estágio** é o estado em que o dispositivo CPE se conecta ao serviço de transporte:
  - **Antes da ativação** significa que o dispositivo CPE faz a conexão com o serviço de transporte antes que o dispositivo CPE seja ativado.
  - **Depois da ativação** significa que o dispositivo CPE faz a conexão com o serviço de transporte depois que o dispositivo CPE é ativado.

  É possível selecionar em que estado o dispositivo CPE estará após o registro ao adicionar um dispositivo CPE.
- **Tipo** é o tipo do serviço de transporte:
  - **P2M**
  - **M2M**
  - **VPN L3**
- **Configurações de conexão** contém informações sobre a interface de serviço criada automaticamente para conectar um dispositivo CPE ao serviço de transporte:
  - Função da interface de serviço:
    - **Folha**
    - **Raiz**

    Só é exibido se o valor na coluna **Tipo** for **P2M**.
  - Tipo de classificação de tráfego na interface de serviço:
    - **Acesso**
    - **VLAN**
    - **Q-in-Q**

- Tag VLAN externa da interface de serviço. Só é exibido se o tipo de classificação de tráfego na interface de serviço for **VLAN** ou **Q-in-Q**.
- Tag VLAN interna da interface de serviço. Só é exibido se o tipo de classificação de tráfego na interface de serviço for **Q-in-Q**.

- **Ações** contém as ações que podem ser executadas com o serviço de transporte.

Adicionar um serviço de transporte a um modelo de CPE

Para adicionar um serviço de transporte a um modelo de CPE:

1. No menu, acesse a subseção **SD-WAN → Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE ao qual deseja adicionar um serviço de transporte.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão ↙↗. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Selecione a guia **Serviços de transporte**.

   Uma tabela de serviços de transporte é exibida.

4. Clique em **+Serviço de transporte**.

5. Na janela aberta, no campo **Nome**, insira o nome do serviço de transporte criado. Se o nome real do serviço de transporte não corresponder ao nome especificado no modelo de CPE, o dispositivo CPE não estabelecerá conexão com o serviço.

6. No campo **Nome do QoS**, insira o nome da regra de qualidade de serviço criada para a interface de serviço, que é criada automaticamente para conectar o dispositivo CPE ao serviço de transporte. Se o nome real da regra de qualidade de serviço não corresponder ao nome especificado no modelo de CPE, a regra não será aplicada à interface de serviço.

7. Na lista suspensa **Estágio**, selecione o estado no qual o dispositivo CPE se conecta ao serviço de transporte:

   - **Antes da ativação** significa que o dispositivo CPE faz a conexão com o serviço de transporte antes que o dispositivo CPE seja ativado.
   - **Depois da ativação** significa que o dispositivo CPE faz a conexão com o serviço de transporte depois que o dispositivo CPE é ativado.

   É possível selecionar em qual estado o dispositivo CPE estará após o registro ao adicionar ou registrar manualmente um dispositivo CPE.

8. Na lista suspensa **Tipo**, selecione o tipo do serviço de transporte:

   - **P2M** Ao selecionar essa opção na lista suspensa **Função**, selecione a função da interface de serviço que é criada automaticamente para conectar o dispositivo CPE ao serviço de transporte:
     - **Folha**
     - **Raiz**

- **M2M**
- **VPN L3** Ao selecionar essa opção, faça o seguinte:
  a. No campo **Endereço IP**, insira o endereço IP da interface L3.
  b. No campo **Máscara**, insira o comprimento do prefixo da interface L3. Intervalo de valores: 0 a 32.

Se o tipo real do serviço de transporte não corresponder ao tipo especificado no modelo de CPE, o dispositivo CPE não estabelecerá conexão com o serviço.

9. Na lista suspensa **Classificação**, selecione o tipo de classificação de tráfego na interface de serviço que é criada automaticamente para conectar o dispositivo CPE ao serviço de transporte:
   - **Acesso** Esse é o nível padrão.
   - **VLAN** Ao selecionar essa opção, no campo **ID da VLAN**, insira a tag VLAN externa da interface de serviço. Intervalo de valores: 1 a 4094.
   - **Q-in-Q** Ao selecionar esse valor, configure a interface L3 que é automaticamente criada e mapeada para a interface de serviço:
     a. No campo **ID da VLAN**, insira a tag VLAN externa da interface de serviço. Intervalo de valores: 1 a 4094.
     b. No campo **ID da VLAN interna**, insira a tag VLAN interna da interface de serviço. Intervalo de valores: 1 a 4094.
10. Clique em **Criar**.
    O serviço de transporte é criado e exibido na tabela.
11. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE.

Editar um serviço de transporte em um modelo de CPE

Para editar um serviço de transporte em um modelo de CPE:

1. No menu, acesse a subseção **SD-WAN → Modelos de CPE**.
   Uma tabela de modelos de CPE é exibida.
2. Clique no modelo de CPE no qual deseja editar um serviço de transporte.
   A área de configurações é exibida. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão↙↗. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.
3. Selecione a guia **Serviços de transporte**.
   Uma tabela de serviços de transporte é exibida.
4. Clique em **Editar** ao lado do serviço de transporte que deseja editar.
5. Na janela aberta, se necessário, edite as configurações do serviço de transporte. Para obter uma descrição das configurações, consulte as instruções para adicionar um serviço de transporte a um modelo de CPE.

6. Clique em **Salvar**.

   O serviço de transporte é modificado e atualizado na tabela.

7. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE.

Excluir um serviço de transporte de um modelo de CPE

Os serviços de transporte excluídos no modelo de CPE não podem ser restaurados.

Para excluir um serviço de transporte em um modelo de CPE:

1. No menu, acesse a subseção **SD-WAN → Modelos de CPE**.

   Uma tabela de modelos de CPE é exibida.

2. Clique no modelo de CPE do qual deseja excluir um serviço de transporte.

   A área de configurações é exibida. É possível expandir a área de configurações para preencher a página inteira clicando no ícone de expansão↙↗. Por padrão, é selecionada a guia **Informações**, que exibe informações gerais sobre o modelo de CPE.

3. Selecione a guia **Serviços de transporte**.

   Uma tabela de serviços de transporte é exibida.

4. Clique em **Excluir** ao lado do serviço de transporte que deseja excluir.

   O serviço de transporte é excluído e não é mais exibido na tabela.

5. Na parte superior da área de configurações, clique em **Salvar** para salvar as configurações do modelo de CPE.

Espelhamento e encaminhamento de tráfego entre dispositivos CPE

O Kaspersky SD-WAN tem suporte ao encaminhamento e espelhamento de tráfego entre dispositivos CPE. É possível redirecionar ou espelhar o tráfego de pontos de coleta de tráfego para o destino do tráfego usando serviços TAP. Encaminhar significa enviar o tráfego que chega aos pontos de coleta de tráfego para o ponto de destino do tráfego, e espelhar significa enviar uma cópia do tráfego.

As interfaces de serviço são usadas como pontos de coleta e destinos de tráfego. Tanto as interfaces de serviço individuais quanto as interfaces de serviço adicionadas a um serviço de transporte podem ser pontos de coleta de tráfego.

É necessário criar um destino de tráfego e, em seguida, especificar esse destino e os pontos de coleta de tráfego ao criar ou editar um serviço TAP. Não é necessário criar pontos de coleta de tráfego com antecedência.

Gerenciar destinos de tráfego

Para visualizar a lista de destinos de tráfego, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador e vá para a seção **Serviços TAP**.

As ações que podem ser executadas com a lista são descritas nas instruções Gerenciar tabelas de componentes da solução.

Criar um destino de tráfego

Para criar um destino de tráfego:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços TAP**.

   Por padrão, é selecionada a guia **Destinos de espelhamento**, que exibe a tabela de destinos de tráfego.

4. Na parte superior da página, clique em **+ Destino de espelhamento**.

5. Na janela aberta, nas listas suspensas **Switch** e **Interface de serviço**, selecione o dispositivo CPE e a interface de serviço criada que deseja usar como o destino de tráfego.

6. Clique em **Criar**.

O destino do tráfego é criado e exibido na tabela.

Excluir um destino de tráfego

Os destinos de tráfego excluídos não podem ser restaurados.

Para excluir um destino de tráfego:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços TAP**.

   Por padrão, é selecionada a guia **Destinos de espelhamento**, que exibe a tabela de destinos de tráfego.

4. Clique em **Excluir** ao lado do destino de tráfego que deseja excluir.

5. Na janela de confirmação, clique em **Excluir**.

O destino do tráfego é excluído e não é mais exibido na tabela.

Gerenciar serviços TAP

Para visualizar a tabela de serviços TAP, vá para a seção **Infraestrutura** do menu, clique em **Gerenciamento** → **Configurações de implementação** ao lado do controlador, vá para a seção **Serviços TAP** e selecione a guia **Serviços TAP**. As informações sobre os serviços TAP são exibidas nas seguintes colunas da tabela:

- **Destino de espelhamento** contém informações sobre a interface de serviço usada como destino do tráfego:
  - Nome e DPID do dispositivo CPE em que a interface de serviço foi criada
  - O número da porta OpenFlow para a qual a interface de serviço é mapeada
- **Espelhar tráfego** indica se o serviço TAP espelha o tráfego dos pontos de coleta de tráfego para o destino do tráfego:
  - **Sim**.
  - **Não**.
- **Tipo** é o tipo de pontos de coleta de tráfego:
  - **SI** significa que interfaces de serviço individuais são usadas como pontos de coleta de tráfego.
  - Se as interfaces de serviço usadas como pontos de coleta de tráfego forem adicionadas a um serviço de transporte, o tipo do serviço de transporte é exibido:
    - **P2P**
    - **Multicast IP**
    - **VPN L3**
    - **P2M**
    - **M2M**
- **Serviço de transporte** é o serviço de transporte ao qual as interfaces de serviço usadas como pontos de coleta de tráfego foram adicionadas. O valor nessa coluna só é exibido se a coluna **Tipo de ponto de origem** estiver exibindo o tipo do serviço de transporte.

- **Pontos de origem** contém informações sobre as interfaces de serviço sendo usadas como pontos de coleta de tráfego:
  - Nomes e DPIDs dos dispositivos CPE em que as interfaces de serviço foram criadas
  - Números de portas OpenFlow para as quais as interfaces de serviço são mapeadas
- **Status** é o status do serviço TAP:
  - **Para cima**
  - **Para baixo**

As ações que podem ser executadas com a tabela são descritas no artigo Gerenciar tabelas de componentes da solução.

Criar um serviço TAP

Para criar um serviço TAP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços TAP**.

   Por padrão, é selecionada a guia **Destinos de espelhamento**, que exibe a tabela de destinos de tráfego.

4. Selecione a guia **Serviços TAP**.

   Uma tabela de serviços TAP é exibida.

5. Na parte superior da página, clique em **+ Serviço TAP**.

6. Caso deseje que o serviço TAP espelhe o tráfego dos pontos de coleta de tráfego para o destino de tráfego, marque a caixa de seleção **Espelhar tráfego**. Quando essa caixa de seleção está marcada, uma cópia do tráfego é enviada ao destino; quando a caixa de seleção está desmarcada, o tráfego é encaminhado. Esta caixa de seleção está desmarcada por padrão.

7. Na lista suspensa **Modo de balanceamento**, selecione o modo de balanceamento para a distribuição do tráfego entre os links:
   - **Por fluxo** significa que os fluxos de tráfego (5-Tuple) são distribuídos entre os links de acordo com o custo do link. Essa é a configuração padrão.
   - **Por pacote** significa que os pacotes de tráfego são distribuídos entre os links de acordo com o custo do link.
   - **Difusão** significa que os pacotes de tráfego são duplicados e transmitidos simultaneamente por todos os links para evitar perdas.

É possível especificar o custo do link manualmente.

8. É possível configurar o modo de balanceamento adaptativo caso deseje que o peso do caminho seja ajustado dinamicamente dependendo do nível de perda de pacotes para o caminho:

   a. Ative o botão **Balanceamento adaptativo**.

   b. No campo **Índice mínimo de perda (%)**, especifique a porcentagem mínima de perda de pacotes no caminho na qual o balanceamento adaptativo começa para ajustar o peso. Intervalo de valores: 0,01 a 100.

   c. No campo **Índice máximo de perda (%)**, especifique a porcentagem máxima de perda de pacotes na qual o caminho é excluído do balanceamento de carga.

   d. Na lista suspensa **Velocidade de convergência**, selecione a taxa de convergência dos pesos adaptativos para os valores calculados:

      - **Rápido**: 1
      - **Rápido**: 0,75
      - **Rápido**: 0,5

9. Na lista suspensa **Destino de espelhamento**, selecione o destino de tráfego criado.

10. Na lista suspensa **Tipo de ponto de origem**, selecione o tipo de ponto de coleta de tráfego:

    - **Interface de serviço** significa que interfaces de serviço individuais são usadas como pontos de coleta de tráfego.
    - **Serviço de transporte** significa que as interfaces de serviço adicionadas a um serviço de transporte são usadas como pontos de coleta de tráfego.

11. Caso tenha selecionado **Serviço de transporte** na lista suspensa **Tipo de ponto de origem**, siga estas etapas:

    a. Na lista suspensa **Tipo**, selecione o tipo do serviço de transporte:

       - **P2P**
       - **Multicast IP**
       - **VPN L3**
       - **P2M**
       - **M2M**

    b. Na lista suspensa **Serviço de transporte**, selecione o serviço de transporte.

12. Na lista suspensa **Pontos de origem**, selecione a interface de serviço criada que deseja usar como ponto de coleta de tráfego.

    O ponto de coleta de tráfego é adicionado e exibido na parte inferior da janela. É possível adicionar vários pontos de coleta de tráfego ou excluir pontos de coleta de tráfego. Para excluir um ponto de coleta de tráfego, clique em **Excluir** ao lado dele.

13. Clique em **Next** e selecione as regras de classificação de tráfego criadas para os pontos de coleta de tráfego.

14. Clique em **Criar**.

O serviço TAP é criado e exibido na tabela.

Visualizar estatísticas de um serviço TAP

Para visualizar as estatísticas de um serviço TAP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços TAP**.

   Por padrão, é selecionada a guia **Destinos de espelhamento**, que exibe a tabela de destinos de tráfego.

4. Selecione a guia **Serviços TAP**.

   Uma tabela de serviços TAP é exibida.

5. Clique em **Gerenciamento** → **Estatísticas** ao lado do serviço TAP cujas estatísticas deseja visualizar.

Isso abre uma janela com estatísticas do serviço TAP.

Editar um serviço TAP

Para editar um serviço TAP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços TAP**.

   Por padrão, é selecionada a guia **Destinos de espelhamento**, que exibe a tabela de destinos de tráfego.

4. Selecione a guia **Serviços TAP**.

   Uma tabela de serviços TAP é exibida.

5. Clique em **Gerenciamento** → **Editar** ao lado do serviço TAP que deseja editar.

6. Na janela aberta, edite as configurações do serviço TAP, se necessário. Para obter uma descrição das configurações, consulte as instruções para criar um serviço TAP.

7. Clique em **Salvar**.

O serviço TAP é modificado e atualizado na tabela.

Excluir um serviço TAP

Os serviços TAP excluídos não podem ser restaurados.

Para excluir um serviço TAP:

1. No menu, acesse a seção **Infraestrutura**.

   A página de gerenciamento de recursos é exibida. Por padrão, é selecionada a guia **Recursos de rede**, que exibe a tabela de controladores.

2. Clique no nome do controlador ou selecione o controlador na tabela e clique em **Configurações de implementação**.

   Isso abre o menu para gerenciar as configurações de implementação do controlador. Por padrão, a seção Nós do controlador, é exibida, mostrando uma tabela de nós do controlador.

3. Vá para a seção **Serviços TAP**.

   Por padrão, é selecionada a guia **Destinos de espelhamento**, que exibe a tabela de destinos de tráfego.

4. Selecione a guia **Serviços TAP**.

   Uma tabela de serviços TAP é exibida.

5. Clique em **Gerenciamento** → **Excluir** ao lado do serviço TAP que deseja excluir.

6. Para excluir as interfaces de serviço adicionadas ao serviço TAP, marque a caixa de seleção **Excluir interfaces de serviço associadas** na janela de confirmação. Esta caixa de seleção está desmarcada por padrão.

7. Clique em **Excluir**.

O serviço TAP é excluído e não é mais exibido na tabela.

Integração com a Kaspersky Unified Monitoring and Analysis Platform

Você pode usar a Kaspersky Unified Monitoring and Analysis Platform (KUMA) para receber notificações sobre eventos de segurança ocorridos no orquestrador e nos dispositivos CPE. Esta seção descreve as etapas para instalar e configurar o KUMA.

O Kaspersky SD-WAN não atua como um agente para o KUMA, mas somente envia eventos ao KUMA sem marcação.

Para instalar o KUMA, você precisa de uma imagem do sistema operacional Astra Linux 1.8.5. Para obter uma lista de sistemas operacionais compatíveis com o KUMA, consulte a Ajuda do KUMA.

Instalação do KUMA

Para instalar o KUMA:

1. Configure o nome do host no servidor no qual você deseja instalar o KUMA:

```
sudo hostnamectl set-hostname kuma.local
```

2. O host deve ter uma lista de servidores DNS. Gerencie-a se necessário:

```
cat /etc/resolv.conf
```

3. No servidor no qual você deseja instalar o KUMA, especifique o endereço IP do servidor no formato `<endereço IP> kuma.local` no arquivo para mapear endereços IP para nomes de domínio:

```
vi /etc/hosts
```

4. Instale os pacotes necessários:

```
sudo yum install python3
sudo pip3 install netaddr
sudo yum install firewalld
sudo yum install compat-openssl11
sudo yum install nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm at-spi2-atk mesa-libgbm alsa-lib
cups-libs libXcomposite libXdamage libXrandr
```

5. Se o servidor usar o mecanismo SELINUX, desative-o definindo `SELINUX=disabled`:

```
vi /etc/selinux/config
```

6. Ative a sincronização de tempo e confirme se está funcionando:

```
sudo systemctl enable --now chronyd sudo timedatectl | grep 'System clock synchronized'
```

7. Se você quiser usar a conta raiz para fazer login no servidor, especifique `PermitRootLogin yes` no arquivo de configuração do SSH:

```
vi /etc/ssh/sshd_config
```

8. Reinicie o servidor.

9. Copie o arquivo com o instalador `kuma-ansible-installer-<número da versão>.tar.gz` no servidor e descompacte-o usando o comando abaixo. Para descompactar o arquivo, você precisará de cerca de 2 GB de espaço em disco.

```
sudo tar -xpf kuma-ansible-installer-<número da versão>.tar.gz
```

10. Mude para o diretório do instalador:

```
cd kuma-ansible-installer
```

11. Copie o modelo `single.inventory.yml.template` e crie um arquivo de inventário denominado `single.inventory.yml` com base no modelo:

```
cp single.inventory.yml.template single.inventory.yml
```

12. Abra o arquivo `single.inventory.yml` para edição.

```
vi single.inventory.yml
```

13. Edite o conteúdo do arquivo seguindo o exemplo abaixo:

```
all:
 vars:
 deploy_to_k8s: false
 need_transfer: false
 deploy_example_services: true
 no_firewall_actions: false
kuma:
 vars:
 ansible_connection: local
 ansible_user: root
 children:
 kuma_core:
 hosts:
 kuma.local:
 raft_node_addr: ""
 kuma_metrics:
 hosts:
 kuma.local:
 kuma_collector:
 hosts:
 kuma.local:
 kuma_correlator:
 hosts:
 kuma.local:
 kuma_storage:
 hosts:
 kuma.local:
 shard: 1
 replica: 1
 keeper: 1
```

14. Prepare o arquivo de chave KUMA.

15. Copie o arquivo de chave para o diretório:

```
sudo cp <key file>.key <diretório do instalador>/roles/kuma/files/license.key
```

16. Execute o instalador:

```
sudo ./install.sh single.inventory.yml
```

Aguarde até que a instalação do KUMA seja concluída.

17. Faça login na interface da Web do KUMA:

    a. No seu navegador, acesse `https://<FQDN do host no qual o KUMA está instalado>:7220`

    b. Insira as credenciais de usuário padrão:

    - nome de usuário: `admin`
    - senha: `mustB3Ch@ng3d!`

18. Altere a senha da conta de admin.

Para obter mais informações sobre a instalação do KUMA, consulte a Ajuda do KUMA.

Cenário: configuração do KUMA

Este cenário descreve o procedimento para configurar a Kaspersky Unified Monitoring and Analysis Platform para integração com o Kaspersky SD-WAN.

O processo de configuração do KUMA envolve as seguintes etapas:

1. **Faça login na interface da Web do KUMA**

   Faça login na interface da Web do KUMA, caso ainda não tenha feito isso. Altere a senha padrão.

2. Configuração do armazenamento
3. Criação e configuração de um normalizador para mensagens do syslog
4. Configurar o correlacionador e as regras de correlação
5. Configuração de um coletor para mensagens do syslog
6. Configurar o serviço de e-mail
7. Configurar regras de notificação

Para obter mais informações sobre como configurar o KUMA, consulte a Ajuda do KUMA.

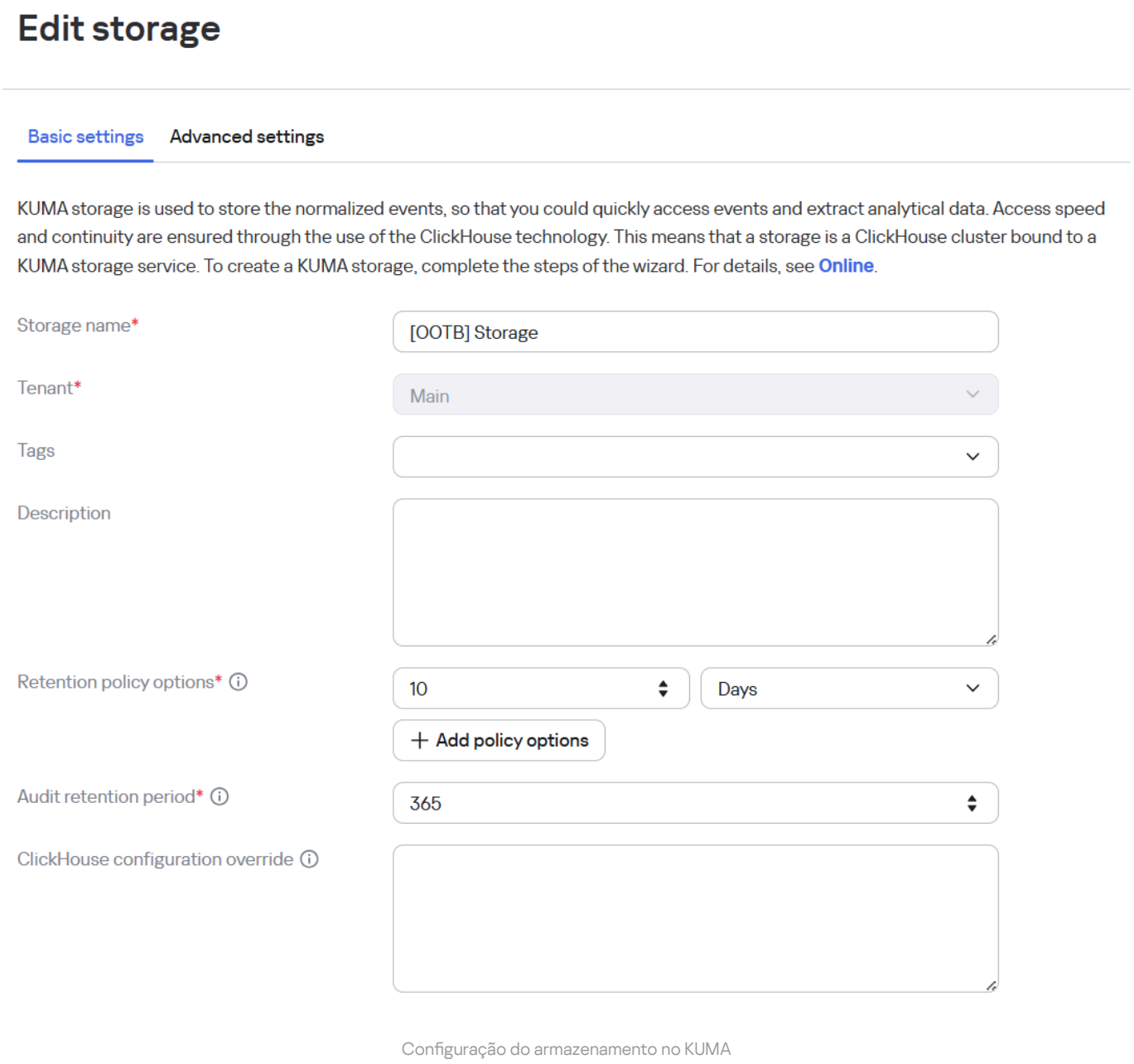
Configuração do armazenamento no KUMA

Por padrão, o `Armazenamento [00TB]` é configurado para reter eventos por no máximo 2 dias. Após esse período, os eventos são excluídos.

Para aumentar o período de retenção:

1. Vá para a seção **Recursos** → **Armazenamentos**.
2. Abra o `Armazenamento [00TB]` criado por padrão.
3. Selecione a guia **Configurações básicas**.
4. Altere a configuração **Opções da política de retenção**.

Você pode especificar o valor em dias, gigabytes ou porcentagem. Defina o valor determinado pela política de segurança da sua empresa (por exemplo, 10 dias).



Configuração do armazenamento no KUMA

5. Salve as alterações clicando no botão **Salvar**.

6. Para aplicar as alterações, atualize as configurações do serviço:

   a. Vá para a seção **Recursos** → **Serviços ativos**.

      O serviço `Armazenamento [OOTB]` é exibido na lista com o status **Atualização necessária**.

   b. Marque a caixa de seleção ao lado do serviço `Armazenamento [OOTB]` e clique em **Atualizar a configuração**.

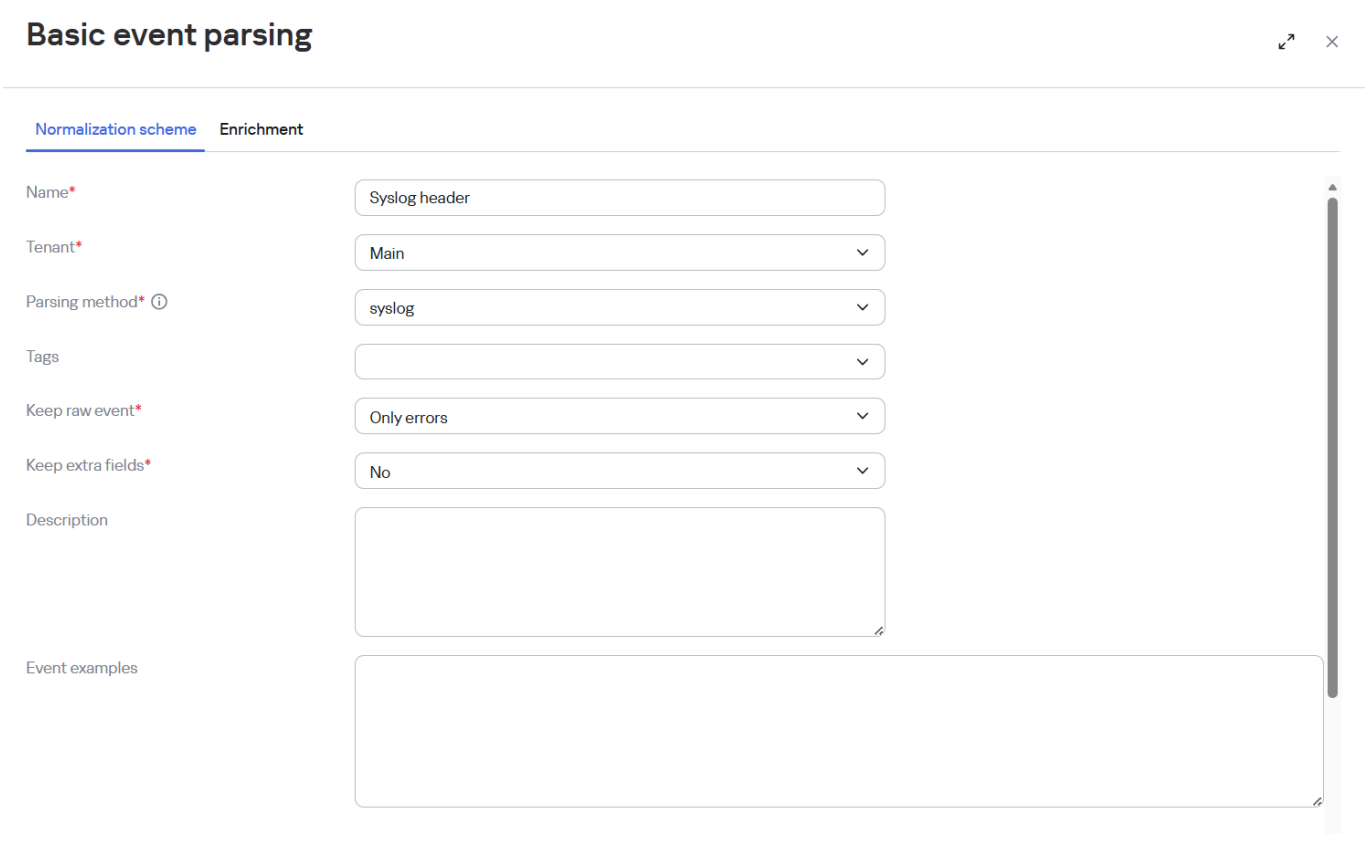
As configurações do serviço são atualizadas sem reinicialização e as alterações entram em vigor.

Criação e configuração de um normalizador no KUMA para mensagens syslog

Para receber mensagens do syslog do orquestrador SD-WAN e CPEs e convertê-las no modelo de dados do KUMA, você precisa criar um normalizador.

Para criar um normalizador:

1. Vá para a seção **Recursos** → **Normalizador**.
2. Clicar em **+ Criar**.
3. Preencha os campos na guia **Esquema de normalização**:
   - No campo **Nome**, insira um nome para o normalizador, por exemplo, `Cabeçalho do syslog`.
   - No campo **Locação**, selecione `Principal`.
   - No campo **Método de análise**, selecione `syslog`.
   - No campo **Manter evento bruto**, selecione `Somente erros`.
   - Em **Manter campos extras**, selecione `Não`.

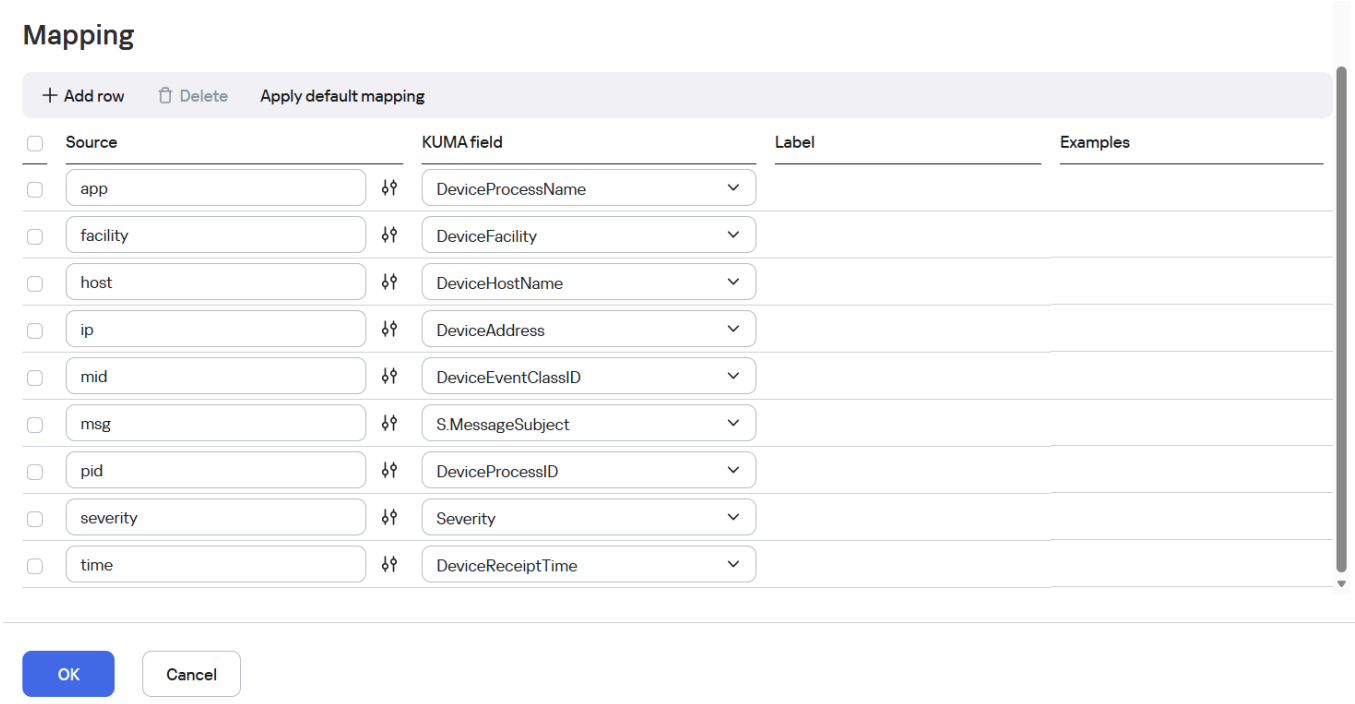


Definir as configurações básicas do normalizador no KUMA

4. Configurar o mapeamento de campos:

   a. Na guia **Esquema de normalização**, em **Mapeamento**, clique em **Aplicar mapeamento padrão**.

   b. Para o valor `msg` no campo **Origem**, altere o valor no campo **KUMA** para `S.MessageSubject` (é compatível com mais caracteres do que o padrão 1024).



Configuração do mapeamento de campo no KUMA

   a. Clique em **OK**.

5. Clique em **Criar**.

As alterações foram salvas.

Configuração do correlacionador e de regras de correlação no KUMA

Para receber notificações de alerta sobre eventos de segurança do orquestrador SD-WAN e CPEs no KUMA, você precisa configurar um correlacionador e regras de correlação.

Um *correlacionador* é um serviço que analisa os eventos recebidos do serviço coletor (Syslog) de acordo com as configurações das regras de correlação e gera uma notificação de evento.

Uma *regra de correlação* é uma regra que descreve o indicador de acionamento e o nível de gravidade atribuído.

Configuração de regras de correlação

Para configurar regras de correlação:

1. Vá para a seção **Recursos** → **Regras de correlação**.
2. Clique em **+ Criar**.
3. Na janela exibida, preencha as configurações da regra de correlação de acordo com a tabela.
4. Selecione a guia **Ações** e ative a regra usando a saída.
5. Repita as etapas para o restante das regras de correlação.

As alterações foram salvas.

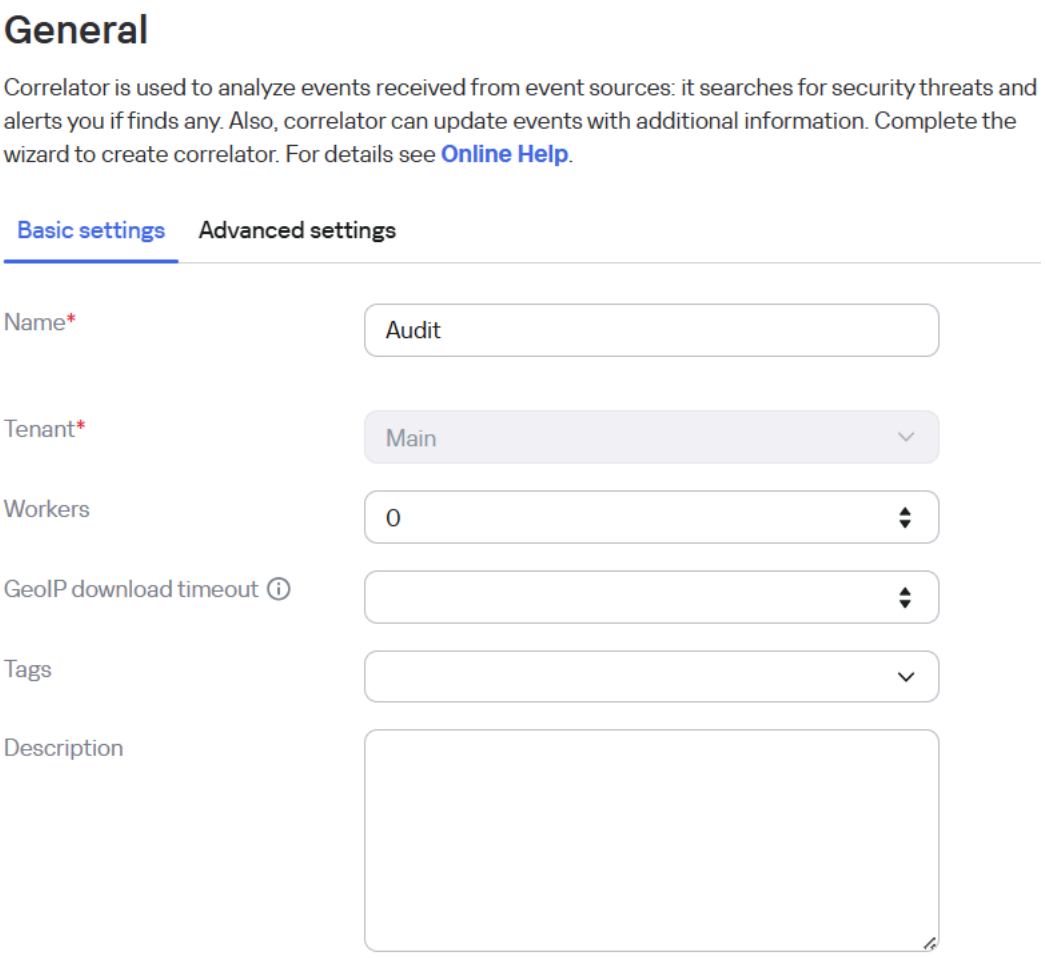
Configuração de um correlacionador

Para configurar um correlacionador:

1. Vá para **Recursos** → **Correlacionadores**.
2. Clique em **+ Criar**.

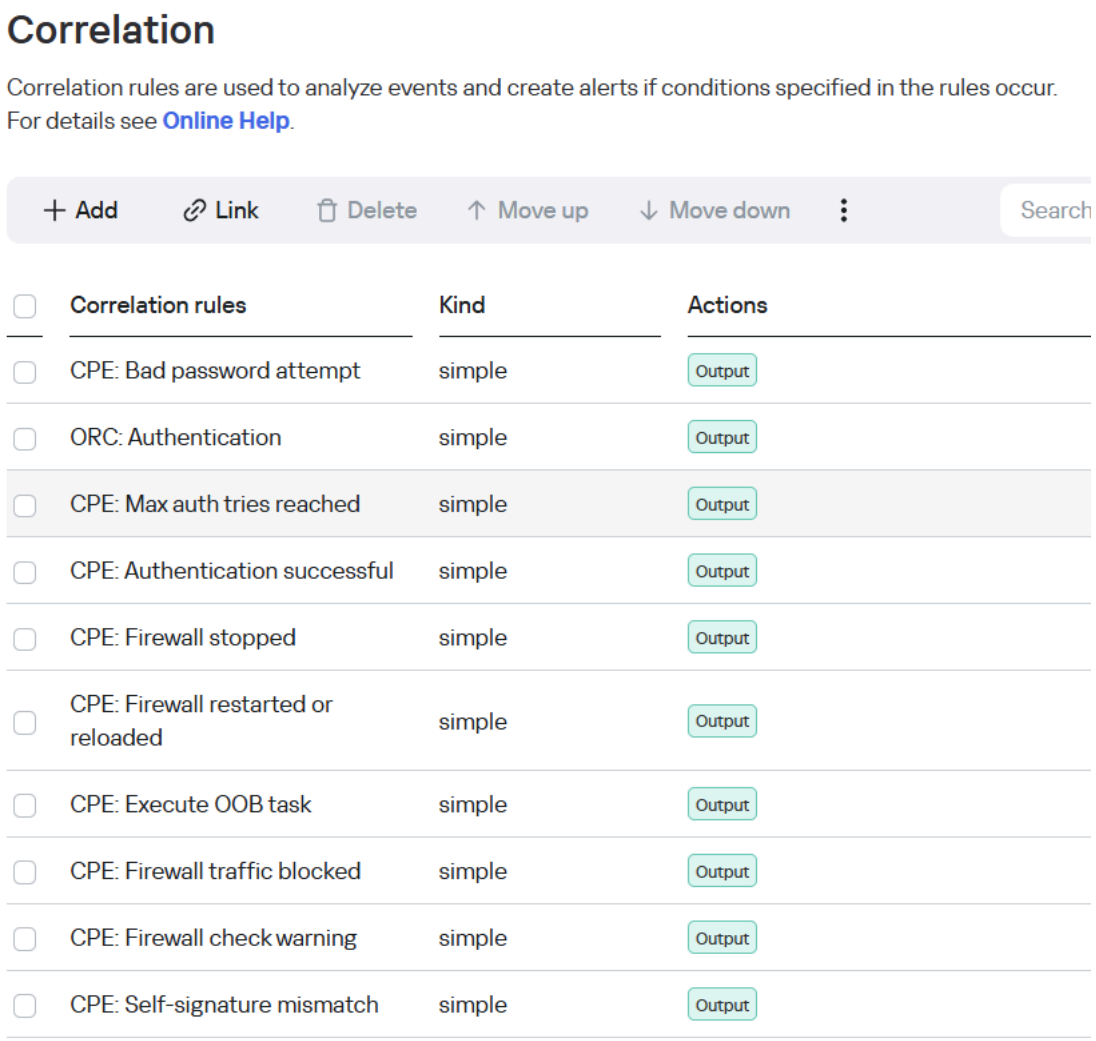
3. Na guia **Geral**, preencha os seguintes campos:

- No campo **Nome**, digite um nome para o correlacionador (por exemplo, `Auditoria`).
- No campo **Locatário**, selecione `Principal` (selecione um locatário diferente, se necessário).



Configurações da correlação na guia **Geral** no KUMA

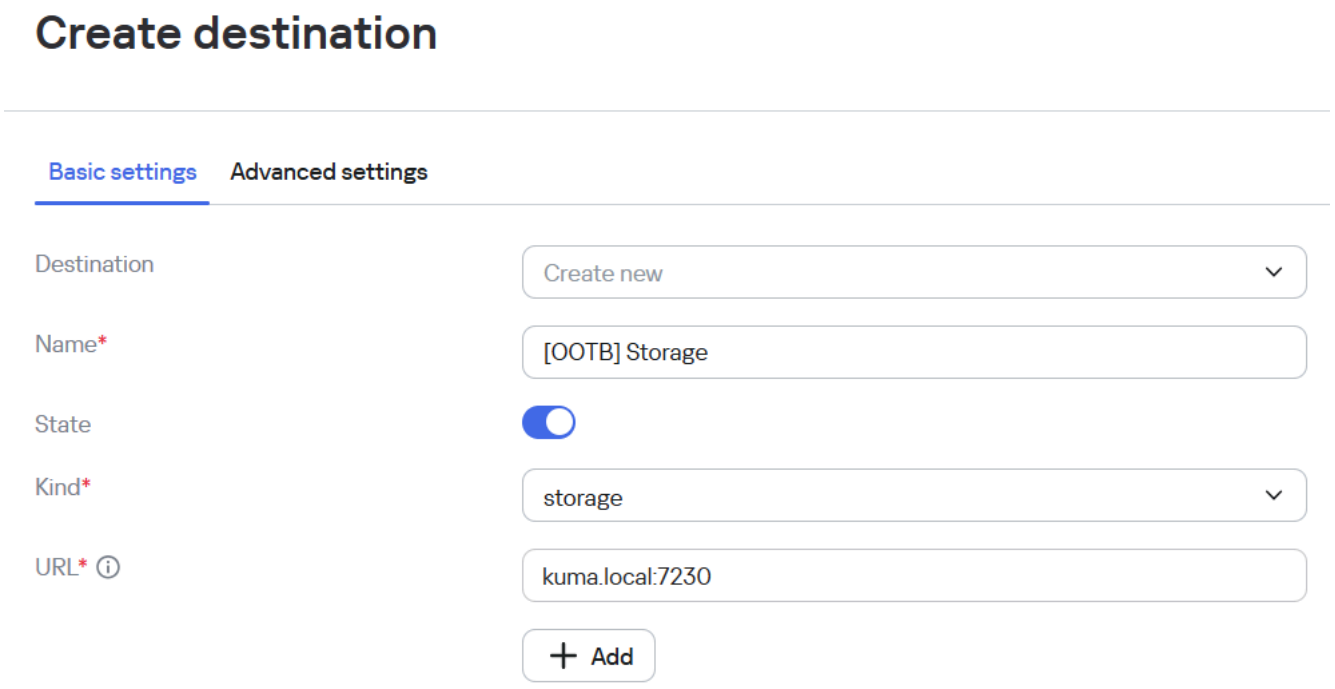
4. Na guia **Correlação**, clique em **Link** e, na janela exibida, selecione todas as regras de correlação já criadas na lista.



Configuração das regras de correlação no correlacionador no KUMA

5. Na guia **Roteamento**, clique em **+ Adicionar** e preencha os campos:

   - No campo **Tipo**, selecione `armazenamento`. Isso faz com que o campo **URL** seja exibido.
   - No campo **URL**, selecione o "Armazenamento [OOTB]" disponível (selecione outro, se necessário).
   - O campo **Nome** é preenchido automaticamente depois que você seleciona uma **URL**.



Configurações do correlacionador na guia **Roteamento** no KUMA

6. Na guia **Validação da instalação**, clique em **Criar e salvar serviço** e obtenha um comando de inicialização que você precisa executar na linha de comando do servidor KUMA.

7. Clique em **Salvar**.

   As alterações foram salvas.

Tabela de referência para criar regras de correlação KUMA

Nome	Tipo	Campos herdados	Nível de importância	Seletores	Ações	Correlacionador
ORC: Audit started	simple	Mensagem	Baixo	Message contain SYS-AUD Started:	Processamento adicional	Auditoria
ORC: Audit stopped	simple	Mensagem	Média	Message contain SYS-AUD Stopped:	Processamento adicional	Auditoria
ORC: CPE Change	simple	Mensagem	Baixo	Message contain SDW-CPE Any:	Processamento adicional	Auditoria
ORC: CPE Change Error	simple	Mensagem	Média	Message contain SDW-CPE AnyError:	Processamento adicional	Auditoria
ORC: CPE Create	simple	Mensagem	Baixo	Message contain SDW-CPE Create:	Processamento adicional	Auditoria
ORC: CPE Create Error	simple	Mensagem	Média	Message contain SDW-CPE CreateError:	Processamento adicional	Auditoria

Nome	Tipo	Campos herdados	Nível de importância	Seletores	Ações	Correlacionador
ORC: CPE Registration	simple	Mensagem	Baixo	Message contain SDW-CPE Registration:	Processamento adicional	Auditoria
ORC: CPE Registration Error	simple	Mensagem	Média	Message contain SDW-CPE RegistrationError:	Processamento adicional	Auditoria
ORC: CPE Delete	simple	Mensagem	Baixo	Message contain SDW-CPE Delete:	Processamento adicional	Auditoria
ORC: CPE Delete Error	simple	Mensagem	Média	Message contain SDW-CPE DeleteError:	Processamento adicional	Auditoria
ORC: CPE Disable	simple	Mensagem	Baixo	Message contain SDW-CPE Disable:	Processamento adicional	Auditoria
ORC: CPE Disable Error	simple	Mensagem	Média	Message contain SDW-CPE DisableError:	Processamento adicional	Auditoria
ORC: CPE Enable	simple	Mensagem	Baixo	Message contain SDW-CPE Enable:	Processamento adicional	Auditoria
ORC: CPE Enable Error	simple	Mensagem	Média	Message contain SDW-CPE EnableError:	Processamento adicional	Auditoria
ORC: CPE Firewall Template	simple	Mensagem	Baixo	Message contain SDW-CPE-GEN FirewallTemplate:	Processamento adicional	Auditoria
ORC: CPE Firewall Template Error	simple	Mensagem	Média	Message contain SDW-CPE-GEN FirewallTemplateError:	Processamento adicional	Auditoria
ORC: CPE Encryption	simple	Mensagem	Baixo	Message contain SDW-CPE-ENC Encryption:	Processamento adicional	Auditoria
ORC: CPE Encryption Error	simple	Mensagem	Média	Message contain SDW-CPE-ENC EncryptionError:	Processamento adicional	Auditoria
ORC: CPE Scripts	simple	Mensagem	Baixo	Message contain SDW-CPE-SCR Scripts:	Processamento adicional	Auditoria
ORC: CPE Scripts Error	simple	Mensagem	Média	Message contain SDW-CPE-SCR ScriptsError:	Processamento adicional	Auditoria
ORC: CPE Interface	simple	Mensagem	Baixo	Message contain SDW-CPE-NET Interface:	Processamento adicional	Auditoria
ORC: CPE Interface Error	simple	Mensagem	Média	Message contain SDW-CPE-NET InterfaceError:	Processamento adicional	Auditoria
ORC: CPE Firewall	simple	Mensagem	Baixo	Message contain SDW-CPE-FW Firewall:	Processamento adicional	Auditoria
ORC: CPE Firewall Error	simple	Mensagem	Média	Message contain SDW-CPE-FW FirewallError:	Processamento adicional	Auditoria
ORC: CPE Static Route	simple	Mensagem	Baixo	Message contain SDW-CPE-STR StaticRoute:	Processamento adicional	Auditoria
ORC: CPE Static Route Error	simple	Mensagem	Média	Message contain SDW-CPE-STR StaticRouteError:	Processamento adicional	Auditoria
ORC: CPE Template Change	simple	Mensagem	Baixo	Message contain SDW-CPET Any:	Processamento adicional	Auditoria
ORC: CPE Template Change Error	simple	Mensagem	Média	Message contain SDW-CPET AnyError:	Processamento adicional	Auditoria
ORC: CPE Template Encryption	simple	Mensagem	Baixo	Message contain SDW-CPET-ENC Encryption:	Processamento adicional	Auditoria
ORC: CPE Template Encryption Error	simple	Mensagem	Média	Message contain SDW-CPET-ENC EncryptionError:	Processamento adicional	Auditoria
ORC: CPE Template Scripts	simple	Mensagem	Baixo	Message contain SDW-CPET-SCR Scripts:	Processamento adicional	Auditoria
ORC: CPE Template Scripts Error	simple	Mensagem	Média	Message contain SDW-CPET-SCR ScriptsError:	Processamento adicional	Auditoria

Nome	Tipo	Campos herdados	Nível de importância	Seletores	Ações	Correlacionador
ORC: CPE Template Interface	simple	Mensagem	Baixo	Message contain SDW-CPET-NET Interface:	Processamento adicional	Auditoria
ORC: CPE Template Interface Error	simple	Mensagem	Média	Message contain SDW-CPET-NET InterfaceError:	Processamento adicional	Auditoria
ORC: CPE Template Static Route	simple	Mensagem	Baixo	Message contain SDW-CPET-STR StaticRoute:	Processamento adicional	Auditoria
ORC: CPE Template Static Route Error	simple	Mensagem	Média	Message contain SDW-CPET-STR StaticRouteError:	Processamento adicional	Auditoria
ORC: Firewall Template	simple	Mensagem	Baixo	Message contain SDW-FWT Firewall:	Processamento adicional	Auditoria
ORC: Firewall Template Error	simple	Mensagem	Média	Message contain SDW-FWT FirewallError:	Processamento adicional	Auditoria
ORC: Zone Template	simple	Mensagem	Baixo	Message contain SDW-FWZ Zone:	Processamento adicional	Auditoria
ORC: Zone Template Error	simple	Mensagem	Média	Message contain SDW-FWZ ZoneError:	Processamento adicional	Auditoria
ORC: Firmware	simple	Mensagem	Baixo	Message contain SDW-FMW Firmware:	Processamento adicional	Auditoria
ORC: Firmware Error	simple	Mensagem	Média	Message contain SDW-FMW FirmwareError:	Processamento adicional	Auditoria
ORC: Firmware Update	simple	Mensagem	Baixo	Message contain SCH-FMWU FirmwareUpdate:	Processamento adicional	Auditoria
ORC: Firmware Update Error	simple	Mensagem	Média	Message contain SCH-FMWU FirmwareUpdateError:	Processamento adicional	Auditoria
ORC: Scheduled Update Settings	simple	Mensagem	Baixo	Message contain SCH-UPDS UpdateSettings:	Processamento adicional	Auditoria
ORC: Scheduled Update Settings Error	simple	Mensagem	Média	Message contain SCH-UPDS UpdateSettingsError:	Processamento adicional	Auditoria
ORC: User Authentication	simple	Mensagem	Baixo	Message contain USR-USR Authentication:	Processamento adicional	Auditoria
ORC: User Authentication Error	simple	Mensagem	Média	Message contain USR-USR AuthenticationError:	Processamento adicional	Auditoria
ORC: User Change	simple	Mensagem	Baixo	Message contain USR-USR UserChange:	Processamento adicional	Auditoria
ORC: User Permission	simple	Mensagem	Baixo	Message contain USR-PERM UserPermissions:	Processamento adicional	Auditoria
ORC: API Call	simple	Mensagem	Baixo	Message contain SYS-API Call:	Processamento adicional	Auditoria
ORC: API Call Complete	simple	Mensagem	Baixo	Message contain SYS-API CallComplete:	Processamento adicional	Auditoria
CPE: Authentication successful	simple	Mensagem	Baixo	DeviceFacility = 10, Severity = 5, Message contains Password auth succeeded	Processamento adicional	Auditoria
CPE: Max auth tries reached	simple	Mensagem	Alto	DeviceFacility = 10, Severity = 6, Message contains Max auth tries reached	Processamento adicional	Auditoria
CPE: Bad password attempt	simple	Mensagem	Média	DeviceFacility = 10 Severity = 4 Message contains Bad password attempt	Processamento adicional	Auditoria

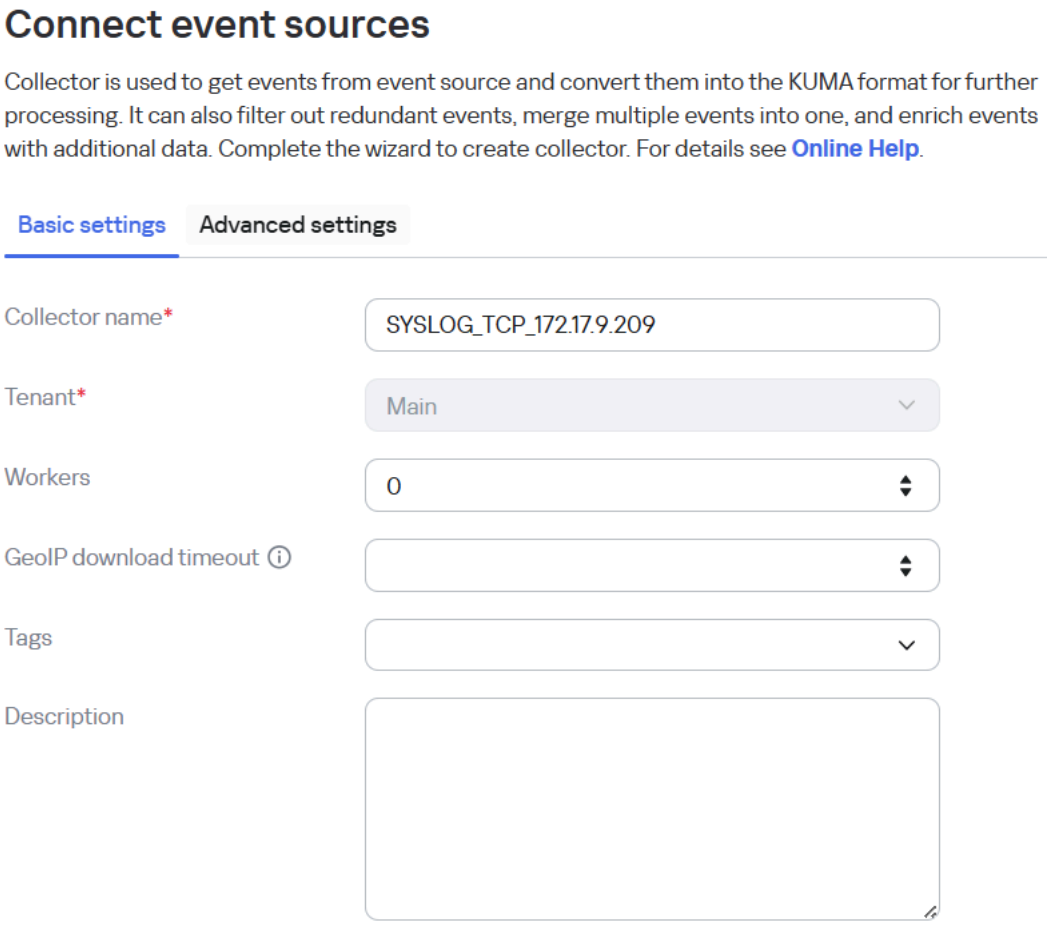
Nome	Tipo	Campos herdados	Nível de importância	Seletores	Ações	Correlacionador
CPE: Execute OOB task	simple	Mensagem	Baixo	DeviceFacility = 1, Severity = 6, Message contains sdwan-oob:	Processamento adicional	Auditoria
CPE: Firewall stopped	simple	Mensagem	Crítico	DeviceFacility = 1, Severity = 2, Message contains Firewall stopped	Processamento adicional	Auditoria
CPE: Firewall started	simple	Mensagem	Baixo	DeviceFacility = 1, Severity = 6, Message contains Firewall started	Processamento adicional	Auditoria
CPE: Firewall restarted or reloaded	simple	Mensagem	Média	DeviceFacility = 1, Severity = 4, OR Message contains Firewall reloaded Message contains Firewall restarted	Processamento adicional	Auditoria
CPE: Firewall audit	simple	Mensagem	Baixo	DeviceFacility = 0, Severity = 6, Message contains FW-AUD	Processamento adicional	Auditoria
CPE: Integrity check successful	simple	Mensagem	Baixo	DeviceFacility = 1, Severity = 6, Message contains Integrity check successful	Processamento adicional	Auditoria
CPE: Integrity check failed	simple	Mensagem	Crítico	DeviceFacility = 1, Severity = 2, Message endsWith Integrity check failed	Processamento adicional	Auditoria
CPE: Verification mismatch	simple	Mensagem	Crítico	DeviceFacility = 1, Severity = 2, Message contains Verification mismatch	Processamento adicional	Auditoria
CPE: Firewall traffic blocked	simple	Mensagem	Crítico	DeviceFacility = 1, Severity = 2,Message contains Integrity check failed. Encaminhamento de tráfego bloqueado	Processamento adicional	Auditoria
CPE: Firewall self-test successful	simple	Mensagem	Baixo	DeviceFacility = 1, Severity = 6, Message contains Successful firewall self test	Processamento adicional	Auditoria
CPE: Firewall self-test failed	simple	Mensagem	Crítico	DeviceFacility = 1, Severity = 2, Message contains Firewall self test failed	Processamento adicional	Auditoria
CPE: USB device inserted	simple	Mensagem	Média	DeviceFacility = 0, Severity = 6, OR Message contains USB deviceMessage contains Storage device detected	Processamento adicional	Auditoria
CPE: USB device mounted	simple	Mensagem	Alto	DeviceFacility = 0, Severity = 6, Message contains mounted filesystem	Processamento adicional	Auditoria
CPE: Time jump detected	simple	Mensagem	Média	DeviceFacility = 3, Severity = 4, Message contains time jump detected	Processamento adicional	Auditoria

Configuração de um coletor para eventos syslog no KUMA

Para receber mensagens do syslog do orquestrador SD-WAN e dos dispositivos CPE, você precisa criar um coletor KUMA.

Para configurar um coletor KUMA:

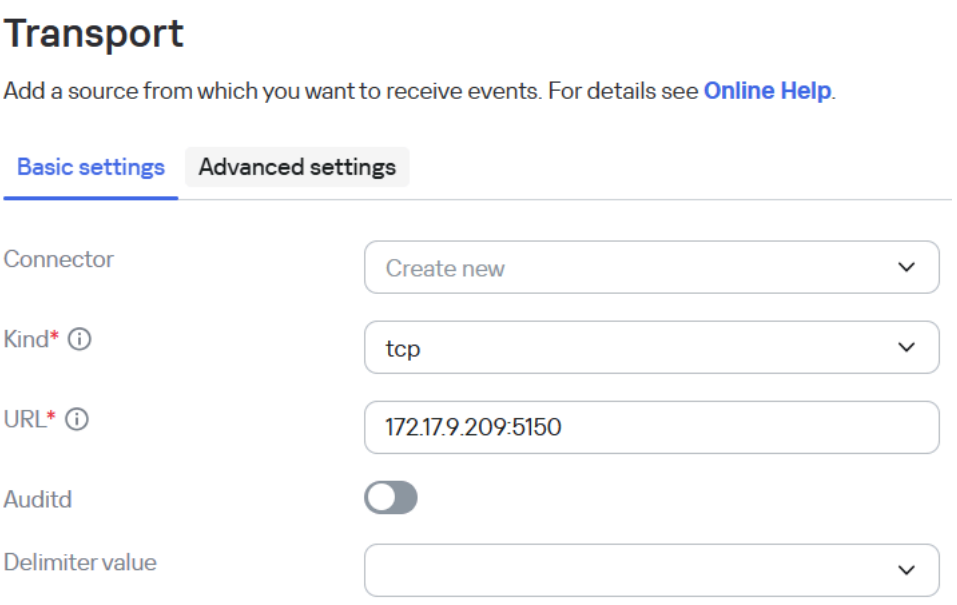
1. Vá para **Recursos** → **Coletores**.
2. Clique em **+ Criar**.
3. Na guia **Conectar fontes de eventos** → **Configurações básicas**, preencha os campos:
   - No campo **Nome do coletor**, insira um nome para o coletor (por exemplo, `SYSLOG_TCP_172.17.9.209`).
   - No campo **Locatário**, selecione `Principal` (selecione um locatário diferente, se necessário).



Configurações do coletor na guia **Conectar fontes de eventos** → **Configurações básicas** no KUMA

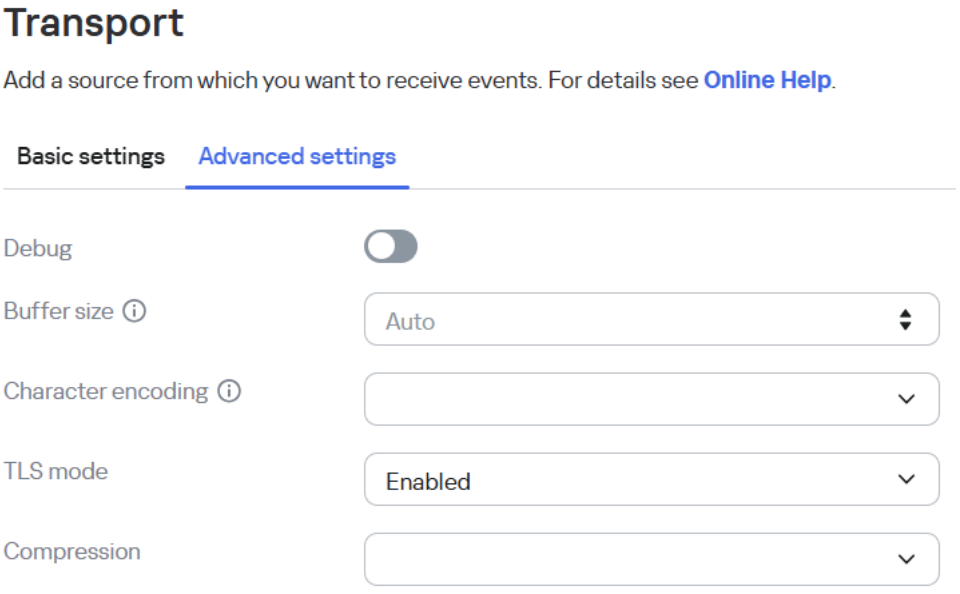
4. Na guia **Transporte** → **Configurações básicas**, preencha os seguintes campos:

   - No campo **Tipo**, selecione `tcp`.
   - No campo **URL**, insira `<endereço IP>:<porta>` (por exemplo, 172.17.9.209:5150).



Configurações do coletor na guia **Transporte** → **Configurações básicas** no KUMA

5. Na guia **Transporte** → **Configurações avançadas**, no campo **Modo TLS**, selecione **Ativado**.

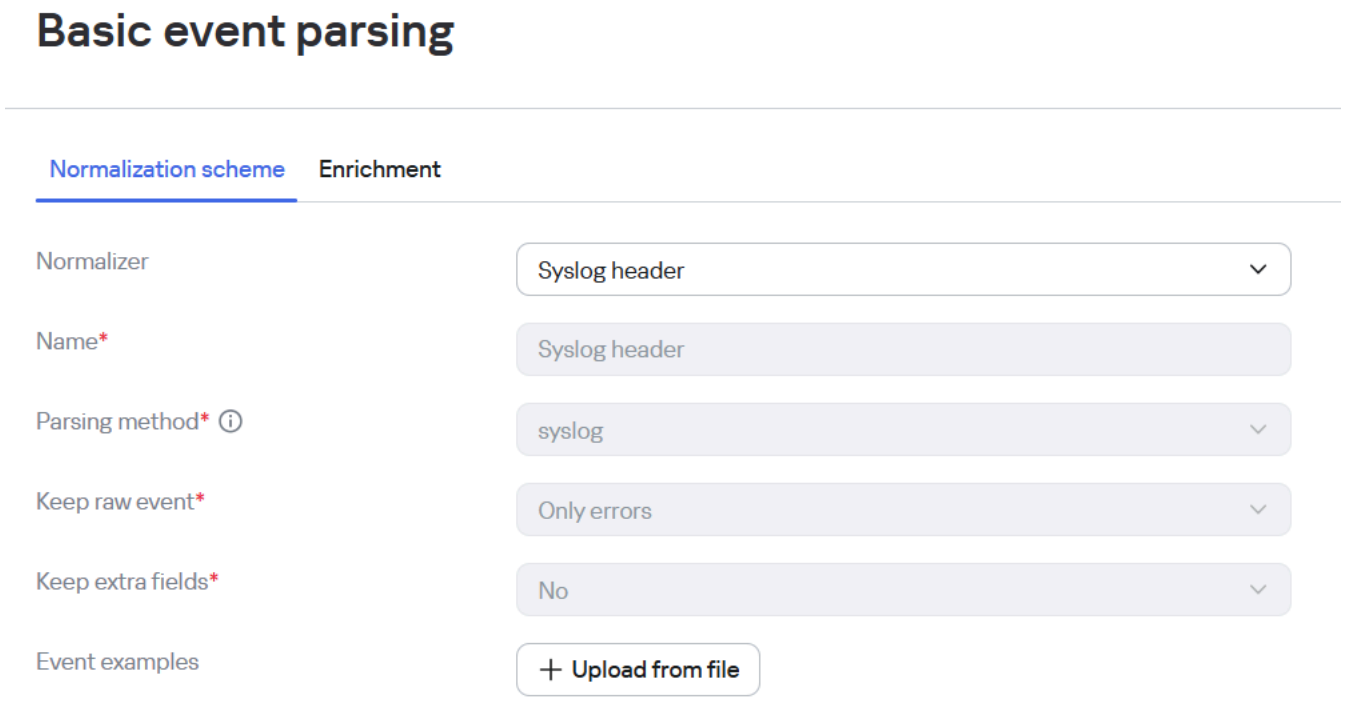


Configurações do coletor na guia **Transporte** → **Configurações avançadas** no KUMA

6. Na guia **Análise de evento** , clique em **+ Adicionar análise de evento** e, no campo **Normalizador**, selecione o modelo de `Cabeçalho do syslog` criado anteriormente.

   O preenchimento dos outros campos é automático.

7. Clique em **OK**.



Configurações do coletor na guia **Análise de eventos** no KUMA

8. Na guia **Roteamento**, clique em **+ Adicionar** e preencha os campos:

   - No campo **Tipo**, selecione `armazenamento`. Isso faz com que o campo **URL** seja exibido.
   - No campo **URL**, selecione o "Armazenamento [OOTB]" disponível (selecione outro, se necessário).
   - O campo **Nome** é preenchido automaticamente depois que você seleciona uma **URL**.

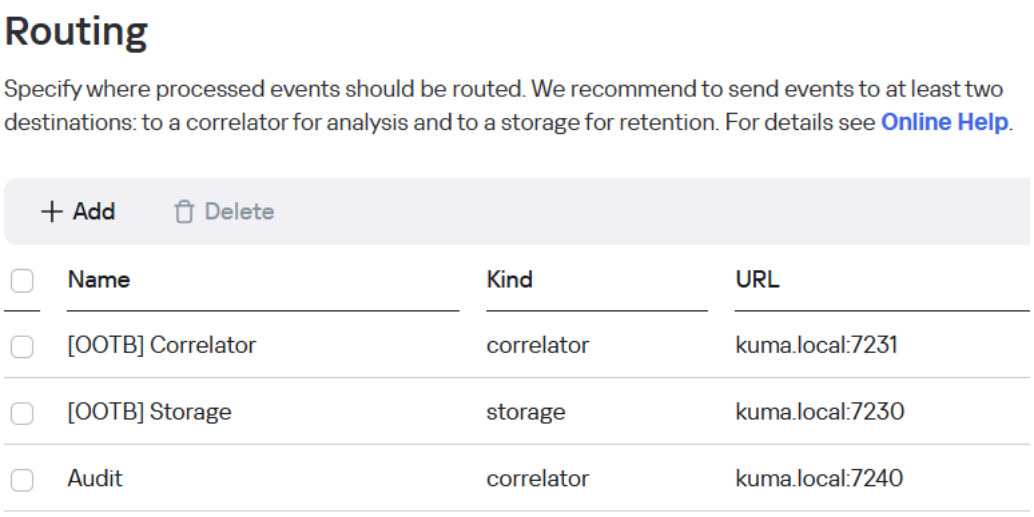
9. Na guia **Roteamento**, clique em **+ Adicionar** e preencha os campos:

   - No campo **Tipo**, selecione `correlacionador`. Isso faz com que o campo **URL** seja exibido.
   - No campo **URL**, selecione um Correlacionador [OOTB] disponível.

     Se o processamento adicional de eventos recebidos for necessário, você precisará configurar o correlacionador de Auditoria. Você pode criar um novo correlacionador mais tarde.
   - O campo **Nome** é preenchido automaticamente depois que você seleciona uma **URL**.

10. Na guia **Roteamento**, clique em **+ Adicionar** e preencha os campos:

    - No campo **Tipo**, selecione `correlacionador`. Isso faz com que o campo **URL** seja exibido.
    - No campo **URL**, selecione `Auditoria`.
    - O campo **Nome** é preenchido automaticamente depois que você seleciona uma **URL**.



Configurações do coletor na guia **Roteamento** no KUMA

11. Na guia **Validação da instalação**, clique em **Criar e salvar serviço** e obtenha um comando de inicialização que você precisa executar na linha de comando do servidor KUMA.

12. Clique em **Salvar**.

    As alterações foram salvas.

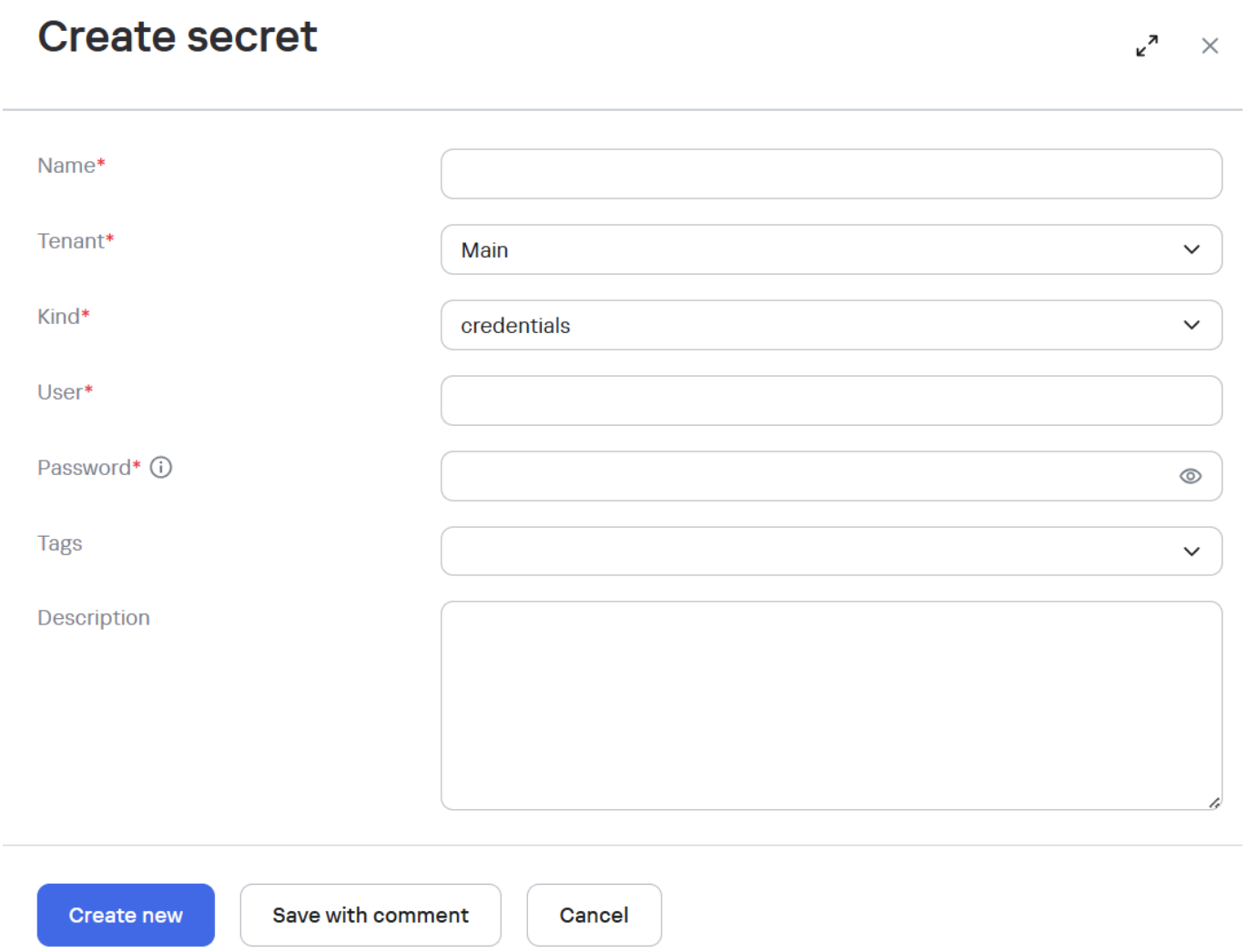
Configuração do serviço de e-mail no KUMA

Para receber notificações por e-mail dos serviços do sistema KUMA e eventos configurados pelo usuário, você precisa configurar um servidor SMTP.

Para configurar o serviço de e-mail:

1. Vá para **Recursos** → **Segredos**.
2. Clique em **+ Criar** e preencha os campos:
    - No campo **Nome**, digite um nome para a política.
    - No campo **Locatário**, selecione `Principal` (selecione um locatário diferente, se necessário).
    - No campo **Tipo**, selecione `credenciais`.
    - No campo **Usuário**, especifique a conta no servidor SMTP.
    - No campo **Senha** , insira a senha da conta no servidor SMTP.

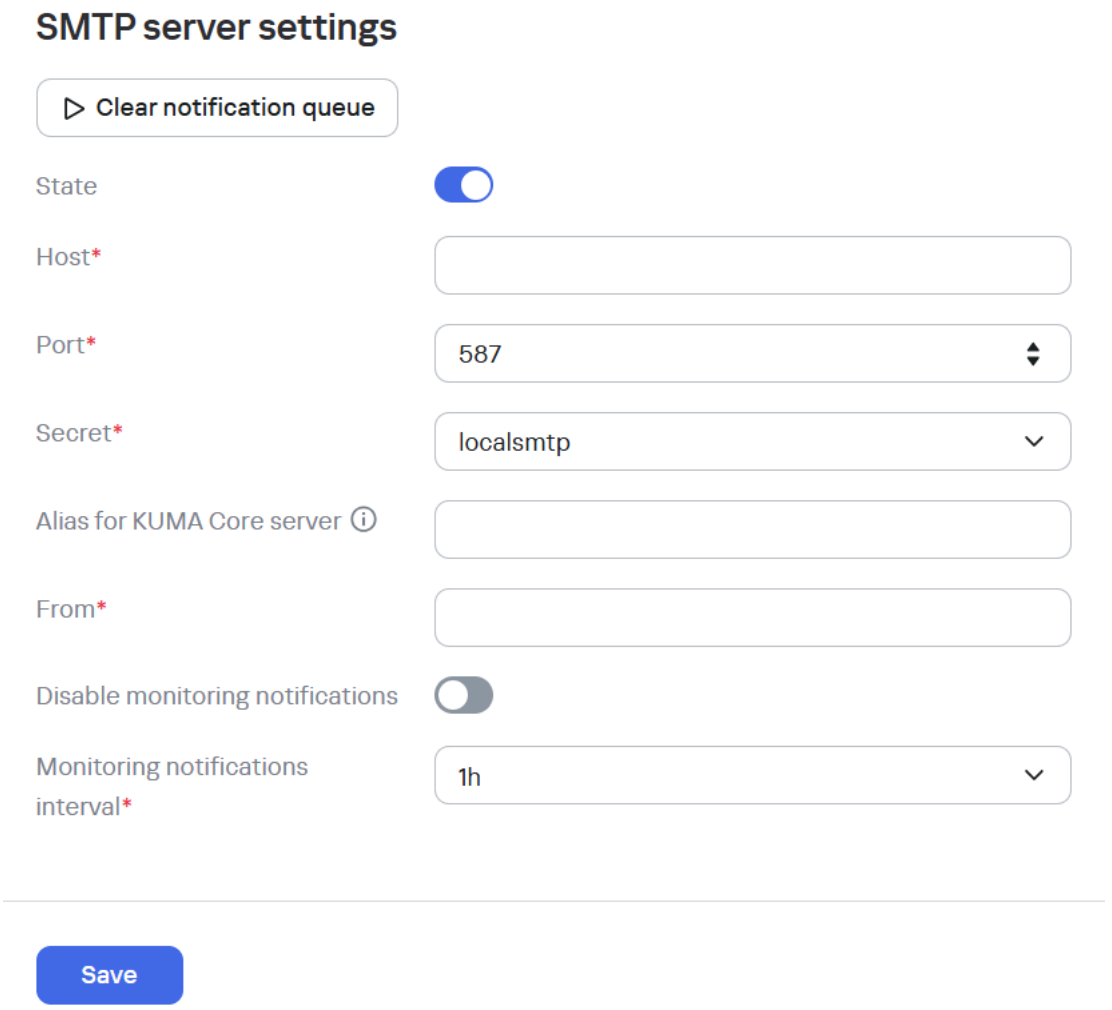
- As **tags** são opcionais.
- A **descrição** é opcional.



Configurações do serviço de e-mail em **Recursos** → **Segredos** no KUMA

3. Vá para a seção **Configurações** → **Outro** → **Comum**.
4. Na seção **Configurações do servidor SMTP**, preencha os seguintes campos:
   - Ative o botão de alternância **Estado**.
   - No campo **Host**, insira o endereço IP ou o FQDN do servidor SMTP.
   - No campo **Porta**, informe a porta do servidor SMTP.
   - No campo **Segredo**, selecione a política configurada anteriormente.
   - O **Alias para o servidor KUMA Core** é opcional.
   - No campo **De**, insira o endereço de e-mail do qual as mensagens serão enviadas ao usuário.

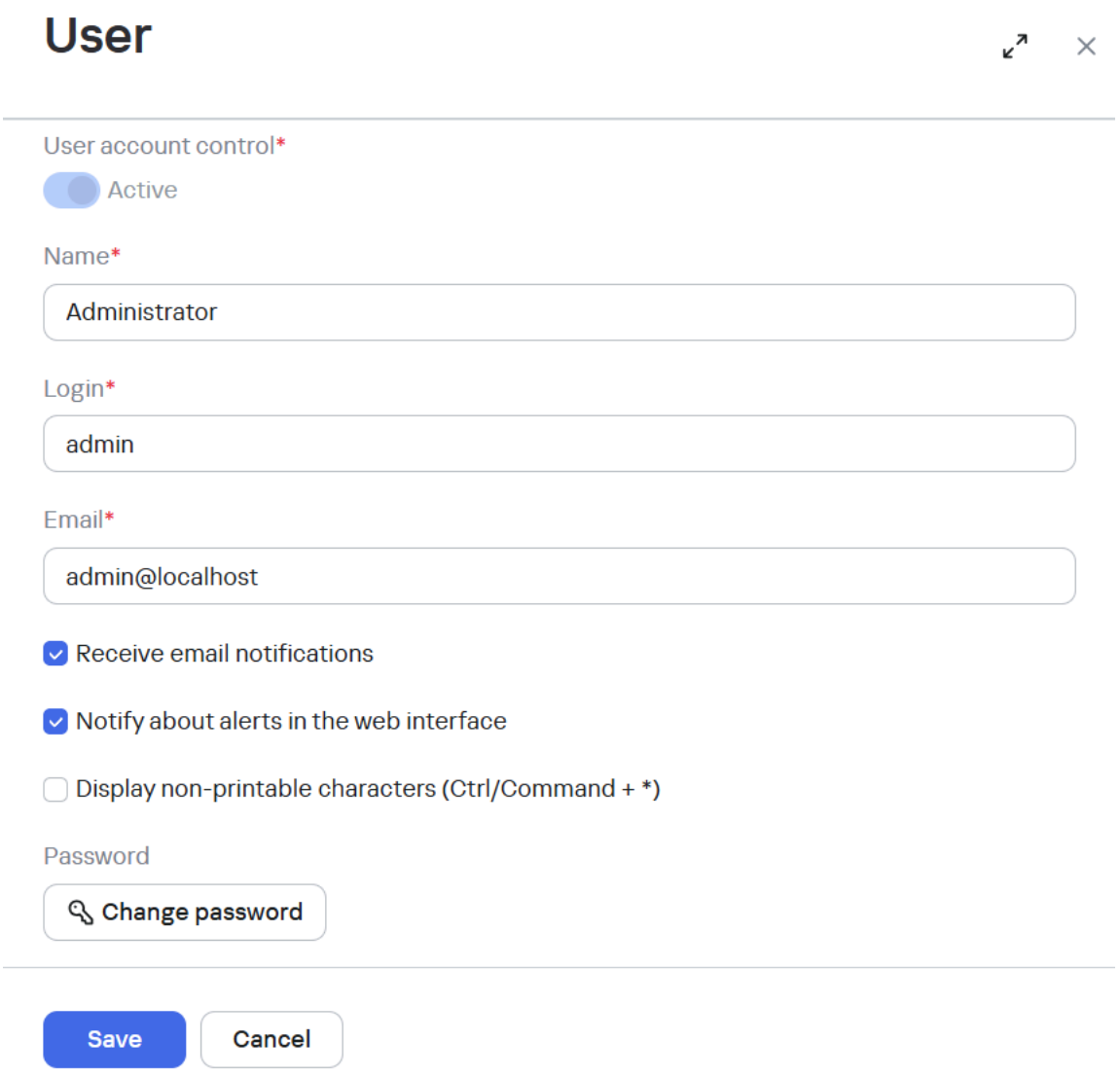
- Deixe o campo **Desativar notificações de monitoramento** inalterado.
- Defina o **Intervalo das notificações de monitoramento** para `1h` (ou um valor diferente, se necessário).



Configurações do serviço de e-mail na seção **Configurações** → **Outro** → **Comum** no KUMA

5. Para ativar o envio de mensagens de e-mail, vá para o Perfil do administrador (**Administrador** → **Perfil**) e preencha os seguintes campos:

   - No campo **E-mail**, insira o endereço de e-mail do Administrador.
   - Marque a caixa de seleção **Receber notificações por e-mail**.
   - Marque a caixa de seleção **Notificar sobre alertas na interface da Web**.



Perfil do administrador no KUMA

As alterações foram salvas.

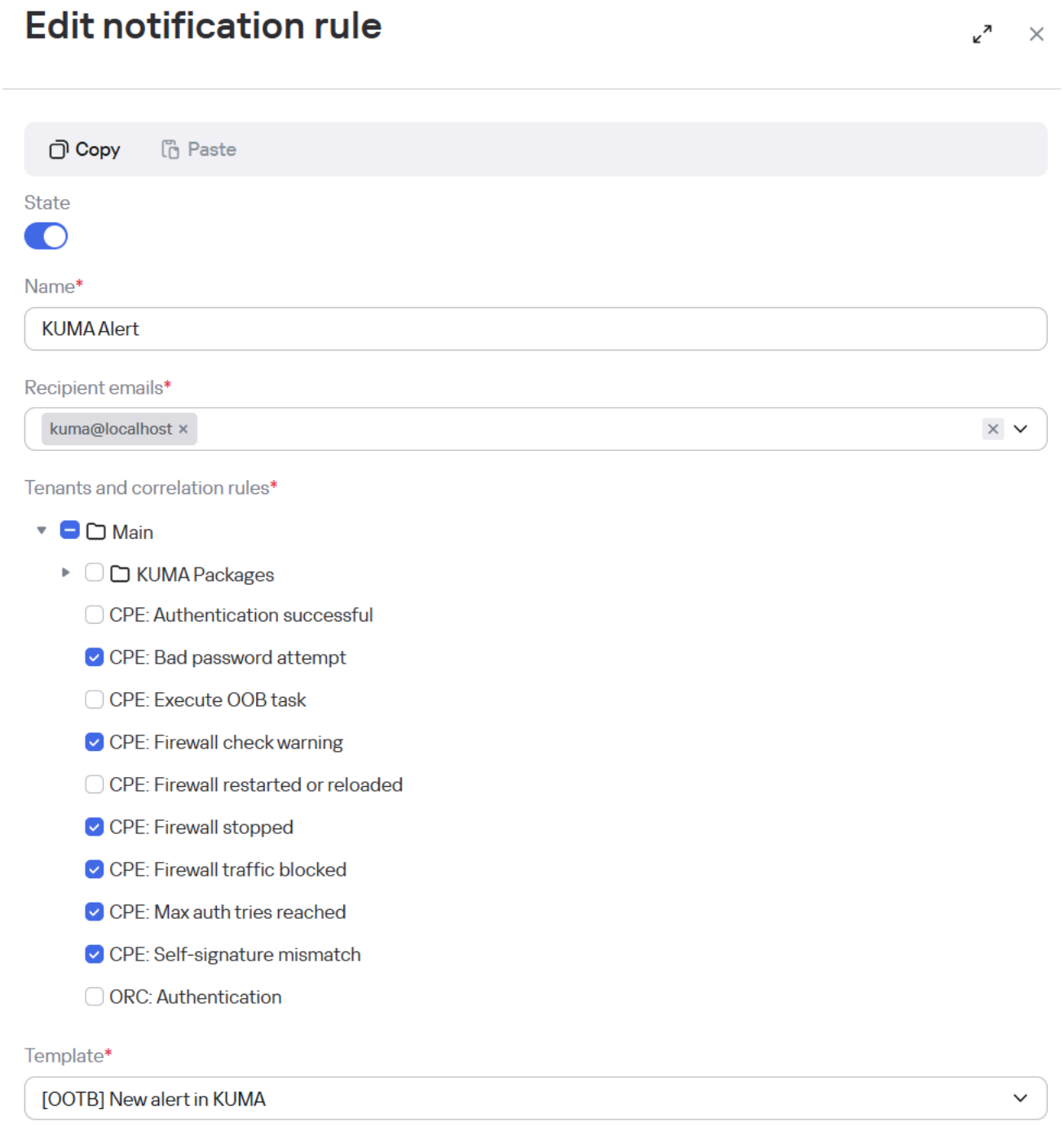
Configuração de regras de notificação no KUMA

Para receber notificações por e-mail do orquestrador SD-WAN e dos CPEs, você precisa configurar as regras de notificação.

Para configurar regras de notificação:

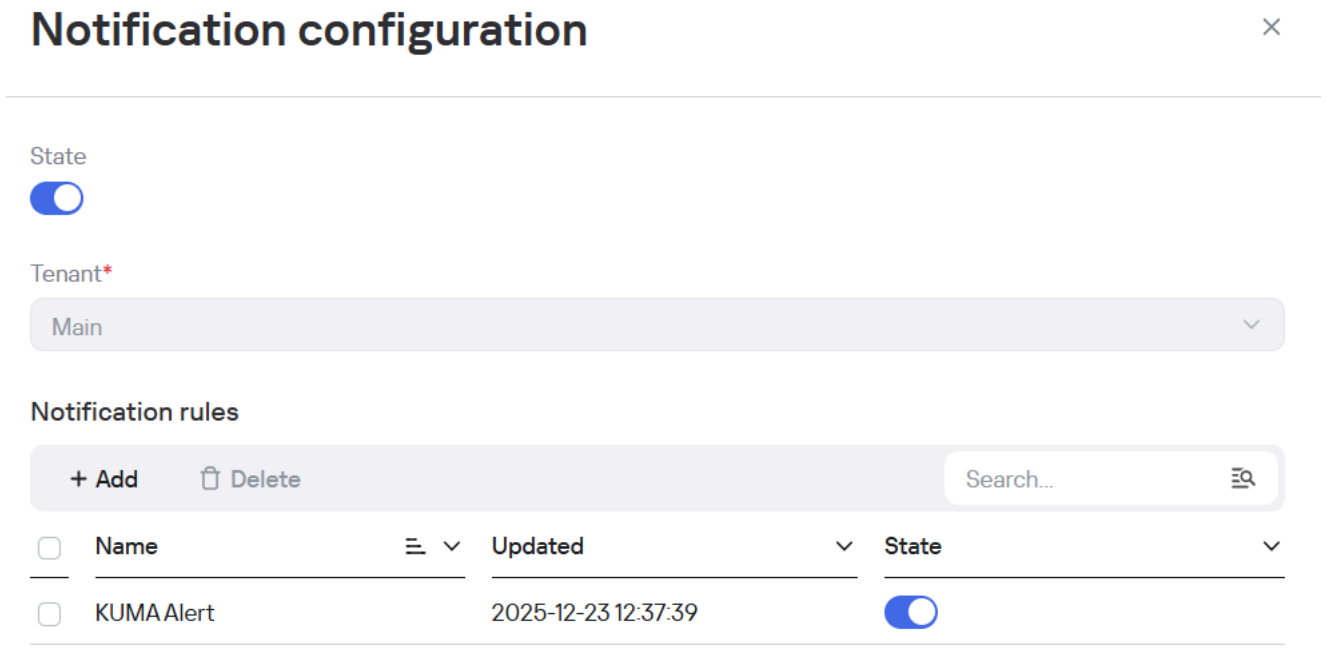
1. Vá para a seção **Configurações** → **Outro** → **Alertas** e selecione a guia **Regras de notificação**
2. Clique em **+ Adicionar configurações para um novo locatário** e preencha os campos.
   - Ative o botão de alternância **Estado**.
   - No campo **Locatário**, selecione `Principal` (selecione um locatário diferente, se necessário).
3. Clique em **+ Adicionar** e preencha os campos:
   - Ative o botão de alternância **Estado**.
   - No campo **Nome**, insira um nome para a regra (por exemplo, "Alerta KUMA").
   - No campo **E-mails do destinatário**, insira os endereços de e-mail dos usuários.
   - Em **Locatários e regras de correlação**, selecione as regras para as quais você deseja receber notificações por e-mail.
   - No campo **Modelo**, selecione o modelo de e-mail padrão `[OOTB] Novo alerta no KUMA` ou crie seus próprios modelos

4. Clique em **Salvar**.



Configurações de regra de notificação no KUMA

5. Clique em **Salvar**.



Configurações de regra de notificação no KUMA

As alterações foram salvas.

Exemplos de configurações para pesquisas por eventos de chave no KUMA

Para pesquisar determinados eventos de segurança, você pode usar uma consulta SQL ao banco de dados (na seção **Eventos** → **Construtor de SQL**). Usando o Construtor de SQL, você pode criar consultas e salvá-las para reutilização rápida.

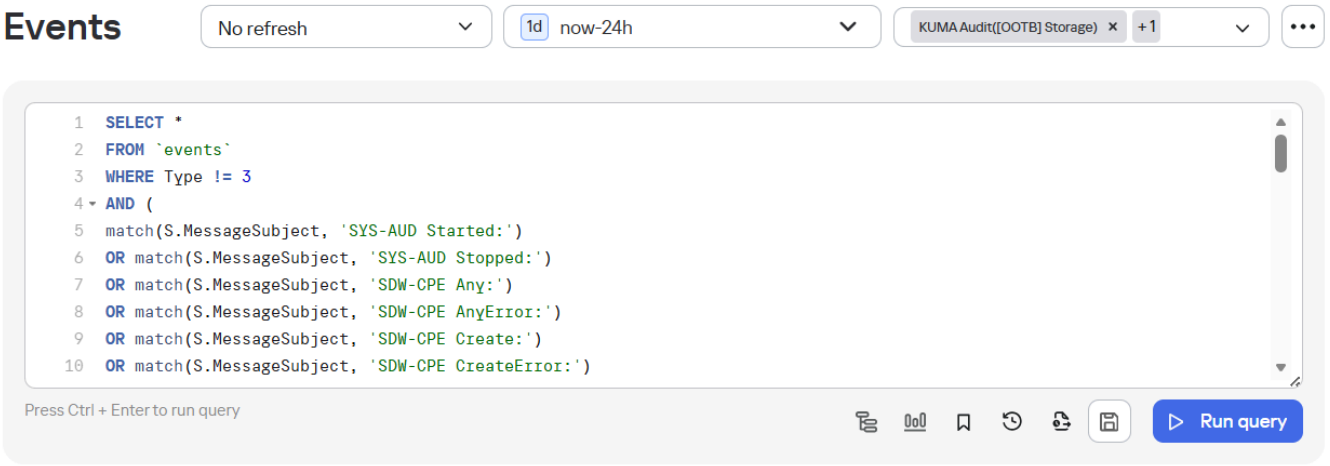
Realização de uma consulta SQL

Para fazer uma consulta SQL:

1. Vá para a seção **Eventos** e localize o campo **Eventos** com a consulta SQL padrão.

2. Exclua o conteúdo da consulta SQL padrão.

3. Copie e cole uma consulta SQL dos exemplos nesta seção.

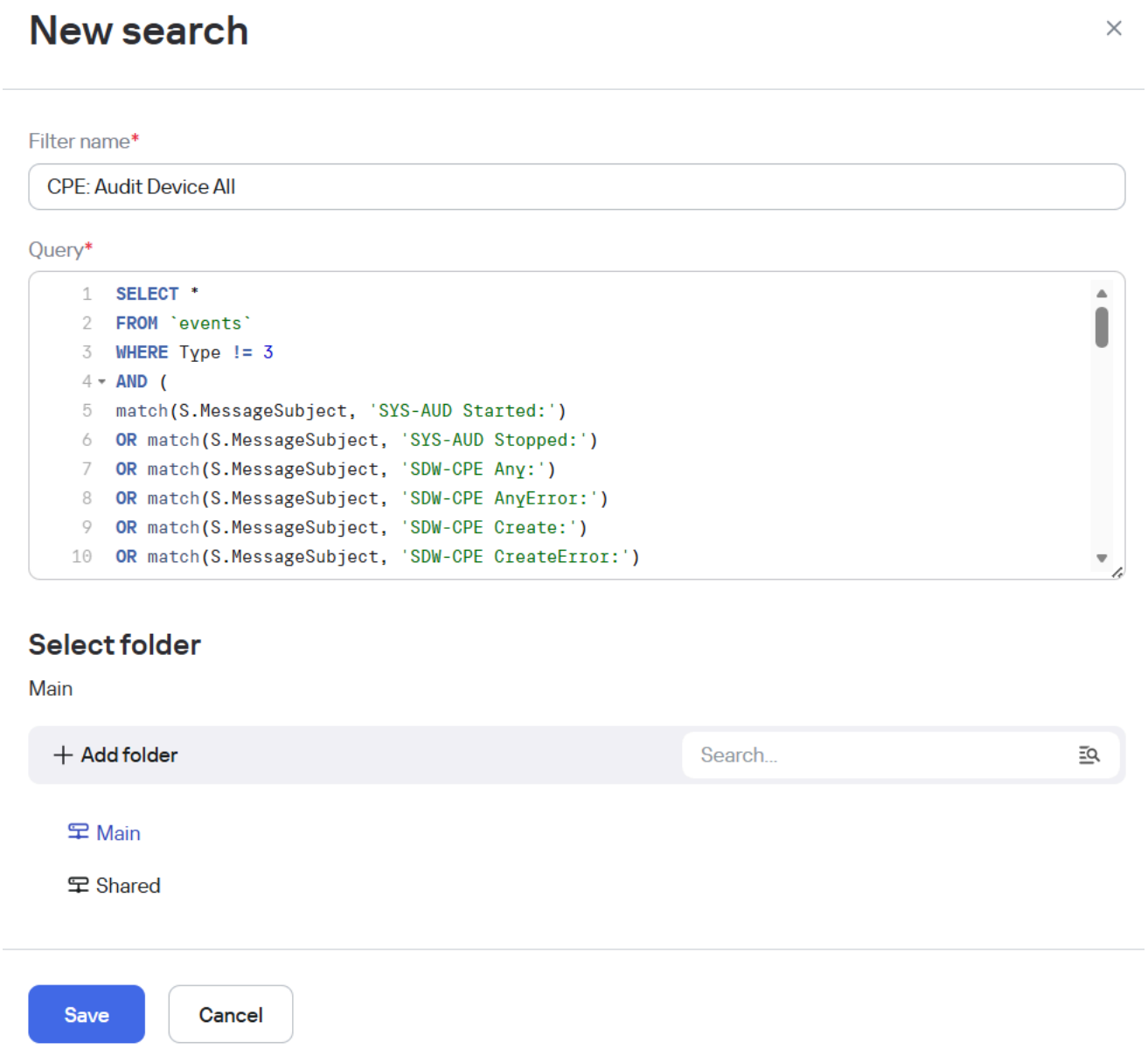


Seção **Eventos** no KUMA

4. Clique em **Salvar filtro atual** e preencha os campos:

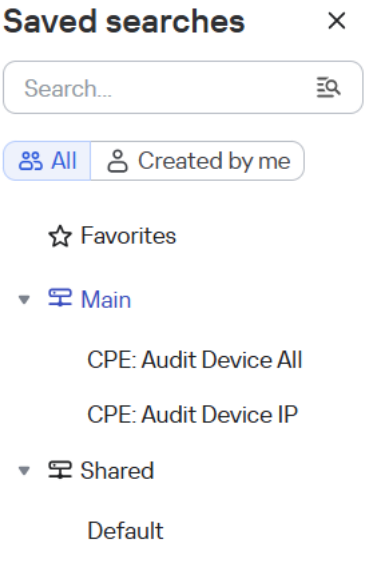
- No campo **Nome do filtro**, insira um nome para a consulta SQL.
- No campo **Consulta**, insira o texto da consulta SQL.
- No campo **Selecionar pasta**, selecione `Principal`.

5. Clique em **Salvar** para salvar a consulta.



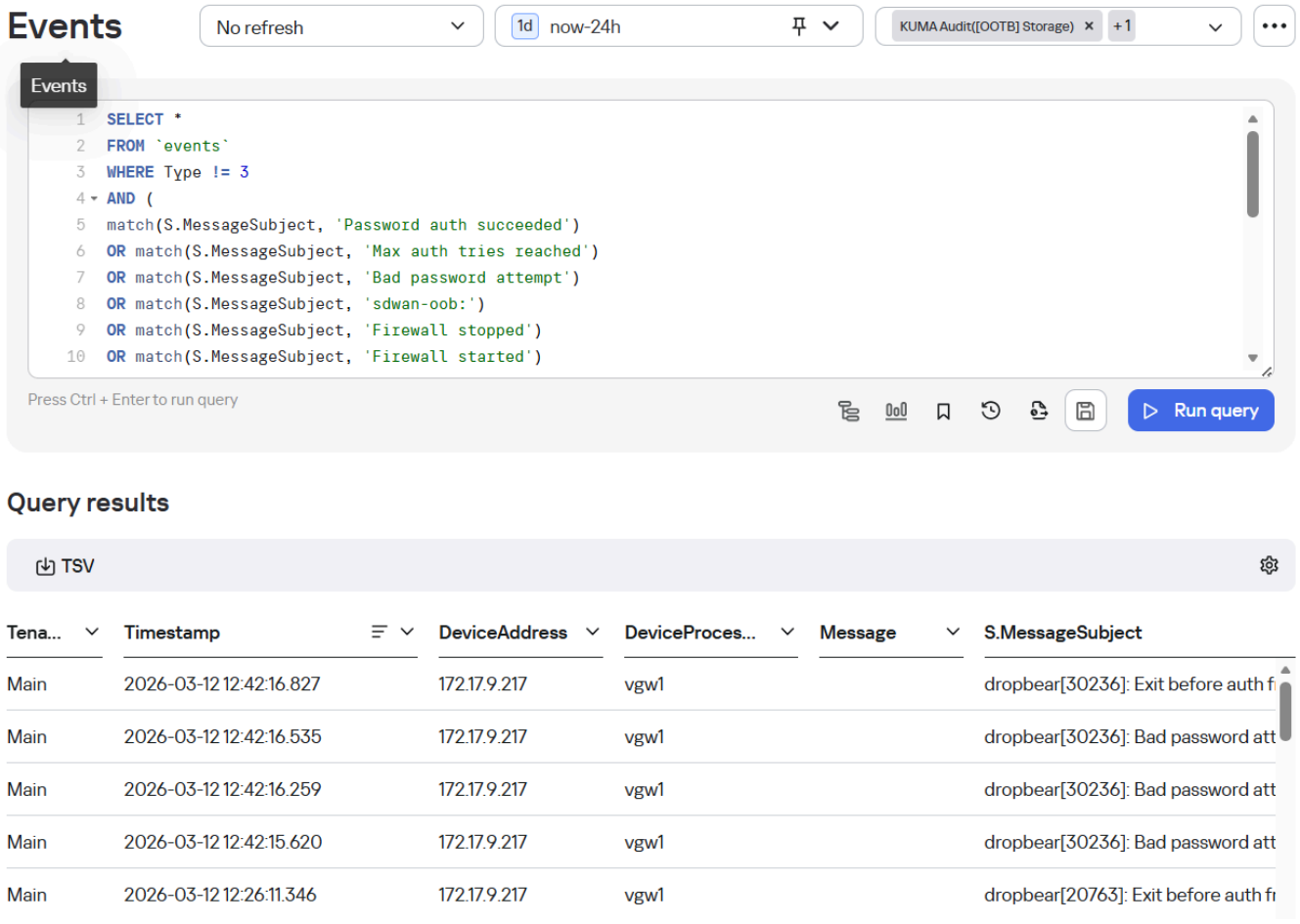
Configurações de consulta SQL no KUMA

6. Clique em **Procuras salvas** para ver as consultas SQL salvas.



Consultas SQL salvas no KUMA

7. Selecione uma consulta SQL e clique em **Executar consulta** para exibir todos os eventos que correspondem à consulta.



Resultado de uma consulta SQL no KUMA

Exemplos de consultas SQL

Nome: ORC: Auditar todas as notificação de segurança

Descrição: serve para pesquisar todos os eventos de segurança no CPE (excluir as regras de correlação que informam sobre a criação do Tipo de alarme != 3)

```
SELECT *
FROM `events`
WHERE Type != 3
AND (
match(S.MessageSubject, 'SYS-AUD Started:')
OR match(S.MessageSubject, 'SYS-AUD Stopped:')
OR match(S.MessageSubject, 'SDW-CPE Any:')
OR match(S.MessageSubject, 'SDW-CPE AnyError:')
OR match(S.MessageSubject, 'SDW-CPE Create:')
OR match(S.MessageSubject, 'SDW-CPE CreateError:')
OR match(S.MessageSubject, 'SDW-CPE Registration:')
OR match(S.MessageSubject, 'SDW-CPE RegistrationError:')
OR match(S.MessageSubject, 'SDW-CPE Delete:')
OR match(S.MessageSubject, 'SDW-CPE DeleteError:')
OR match(S.MessageSubject, 'SDW-CPE Disable:')
OR match(S.MessageSubject, 'SDW-CPE DisableError:')
OR match(S.MessageSubject, 'SDW-CPE Enable:')
OR match(S.MessageSubject, 'SDW-CPE EnableError:')
OR match(S.MessageSubject, 'SDW-CPE-GEN FirewallTemplate:')
OR match(S.MessageSubject, 'SDW-CPE-GEN FirewallTemplateError:')
OR match(S.MessageSubject, 'SDW-CPE-ENC Encryption:')
OR match(S.MessageSubject, 'SDW-CPE-ENC EncryptionError:')
OR match(S.MessageSubject, 'SDW-CPE-SCR Scripts:')
OR match(S.MessageSubject, 'SDW-CPE-SCR ScriptsError:')
OR match(S.MessageSubject, 'SDW-CPE-NET Interface:')
OR match(S.MessageSubject, 'SDW-CPE-NET InterfaceError:')
OR match(S.MessageSubject, 'SDW-CPE-FW Firewall:')
OR match(S.MessageSubject, 'SDW-CPE-FW FirewallError:')
OR match(S.MessageSubject, 'SDW-CPE-STR StaticRoute:')
OR match(S.MessageSubject, 'SDW-CPE-STR StaticRouteError:')
OR match(S.MessageSubject, 'SDW-CPET Any:')
OR match(S.MessageSubject, 'SDW-CPET AnyError:')
OR match(S.MessageSubject, 'SDW-CPET-ENC Encryption:')
OR match(S.MessageSubject, 'SDW-CPET-ENC EncryptionError:')
OR match(S.MessageSubject, 'SDW-CPET-SCR Scripts:')
OR match(S.MessageSubject, 'SDW-CPET-SCR ScriptsError:')
OR match(S.MessageSubject, 'SDW-CPET-NET Interface:')
OR match(S.MessageSubject, 'SDW-CPET-NET InterfaceError:')
OR match(S.MessageSubject, 'SDW-CPET-STR StaticRoute:')
OR match(S.MessageSubject, 'SDW-CPET-STR StaticRouteError:')
OR match(S.MessageSubject, 'SDW-FWT Firewall:')
OR match(S.MessageSubject, 'SDW-FWT FirewallError:')
OR match(S.MessageSubject, 'SDW-FWZ Zone:')
OR match(S.MessageSubject, 'SDW-FWZ ZoneError:')
OR match(S.MessageSubject, 'SDW-FMW Firmware:')
OR match(S.MessageSubject, 'SDW-FMW FirmwareError:')
OR match(S.MessageSubject, 'SCH-FMWU FirmwareUpdate:')
OR match(S.MessageSubject, 'SCH-FMWU FirmwareUpdateError:')
OR match(S.MessageSubject, 'SCH-UPDS UpdateSettings:')
OR match(S.MessageSubject, 'SCH-UPDS UpdateSettingsError:')
OR match(S.MessageSubject, 'USR-USR Authentication:')
OR match(S.MessageSubject, 'USR-USR AuthenticationError:')
OR match(S.MessageSubject, 'USR-USR UserChange:')
OR match(S.MessageSubject, 'USR-PERM UserPermissions:')
OR match(S.MessageSubject, 'SYS-API Call:')
OR match(S.MessageSubject, 'SYS-API CallComplete:')
)
ORDER BY Timestamp DESC
LIMIT 500;
```

Nome: CPE: auditar todos os dispositivos

Descrição: encontrar todos os eventos de segurança no CPE

```
SELECT *
FROM `events`
WHERE Type != 3
AND (
match(S.MessageSubject, 'Password auth succeeded')
OR match(S.MessageSubject, 'Max auth tries reached')
OR match(S.MessageSubject, 'Bad password attempt')
OR match(S.MessageSubject, 'sdwan-oob:')
OR match(S.MessageSubject, 'Firewall stopped')
OR match(S.MessageSubject, 'Firewall started')
OR match(S.MessageSubject, 'Firewall reloaded')
OR match(S.MessageSubject, 'Firewall restarted')
OR match(S.MessageSubject, 'FW-AUD')
OR match(S.MessageSubject, 'Integrity check successful')
OR match(S.MessageSubject, 'Integrity check failed')
OR match(S.MessageSubject, 'Verification mismatch')
OR match(S.MessageSubject, 'Traffic forwarding blocked')
OR match(S.MessageSubject, 'Successful firewall self test')
OR match(S.MessageSubject, 'Firewall self test failed')
OR match(S.MessageSubject, 'USB device')
OR match(S.MessageSubject, 'Storage device detected')
OR match(S.MessageSubject, 'mounted filesystem')
OR match(S.MessageSubject, 'time jump detected')
)
ORDER BY Timestamp DESC
LIMIT 500;
```

Nome: CPE: Auditar todos os IPs dos dispositivos

Descrição: localiza todos os eventos de segurança no CPE com base em um endereço IP específico

```
SELECT *
FROM `events`
WHERE DeviceAddress = '172.17.9.223' AND Type != 3
AND (
match(S.MessageSubject, 'Password auth succeeded')
OR match(S.MessageSubject, 'Max auth tries reached')
OR match(S.MessageSubject, 'Bad password attempt')
OR match(S.MessageSubject, 'sdwan-oob:')
OR match(S.MessageSubject, 'Firewall stopped')
OR match(S.MessageSubject, 'Firewall started')
OR match(S.MessageSubject, 'Firewall reloaded')
OR match(S.MessageSubject, 'Firewall restarted')
OR match(S.MessageSubject, 'FW-AUD')
OR match(S.MessageSubject, 'Integrity check successful')
OR match(S.MessageSubject, 'Integrity check failed')
OR match(S.MessageSubject, 'Verification mismatch')
OR match(S.MessageSubject, 'Traffic forwarding blocked')
OR match(S.MessageSubject, 'Successful firewall self test')
OR match(S.MessageSubject, 'Firewall self test failed')
OR match(S.MessageSubject, 'USB device')
OR match(S.MessageSubject, 'Storage device detected')
OR match(S.MessageSubject, 'mounted filesystem')
OR match(S.MessageSubject, 'time jump detected')
)
ORDER BY Timestamp DESC
LIMITE 500
```

Integração com o Kaspersky CyberSecurity for Networks

É possível integrar o Kaspersky SD-WAN ao Kaspersky Industrial CyberSecurity for Networks para encaminhar o tráfego SPAN das interfaces de serviço dos dispositivos CPE para as interfaces de rede dos nós do Kaspersky Industrial CyberSecurity for Networks. Antes de configurar a integração, ative a criptografia de tráfego em dispositivos CPE de cujas interfaces de serviço se deseja encaminhar o tráfego SPAN. Recomendamos colocar os dispositivos CPE em uma rede dedicada do Kaspersky Industrial CyberSecurity

https://support.kaspersky.com/help/KICSforNetworks/4.2/en-US/102350.htm

.

O tráfego SPAN é identificado por tags VLAN adicionadas aos pacotes de tráfego de acordo com o padrão IEEE 802.1q. Certifique-se de que as tags VLAN correspondentes sejam usadas nas interfaces de serviço dos dispositivos CPE e nas interfaces de rede dos nós do Kaspersky Industrial CyberSecurity for Networks.

Para uma integração eficaz do Kaspersky SD-WAN com o Kaspersky Industrial CyberSecurity for Networks, é possível aumentar o limite do número de pontos de monitoramento configurando também componentes do Kaspersky Industrial CyberSecurity for Networks. Limites máximos possíveis:

- Até 100 pontos de monitoramento em um nó do Kaspersky Industrial CyberSecurity for Networks
- Até 100 pontos de monitoramento no total no nó do Kaspersky Industrial CyberSecurity for Networks

O restante dos requisitos para a implementação dos componentes do Kaspersky Industrial CyberSecurity for Networks são semelhantes a outros cenários de implementação, por exemplo, a instalação de um servidor sem sensores externos

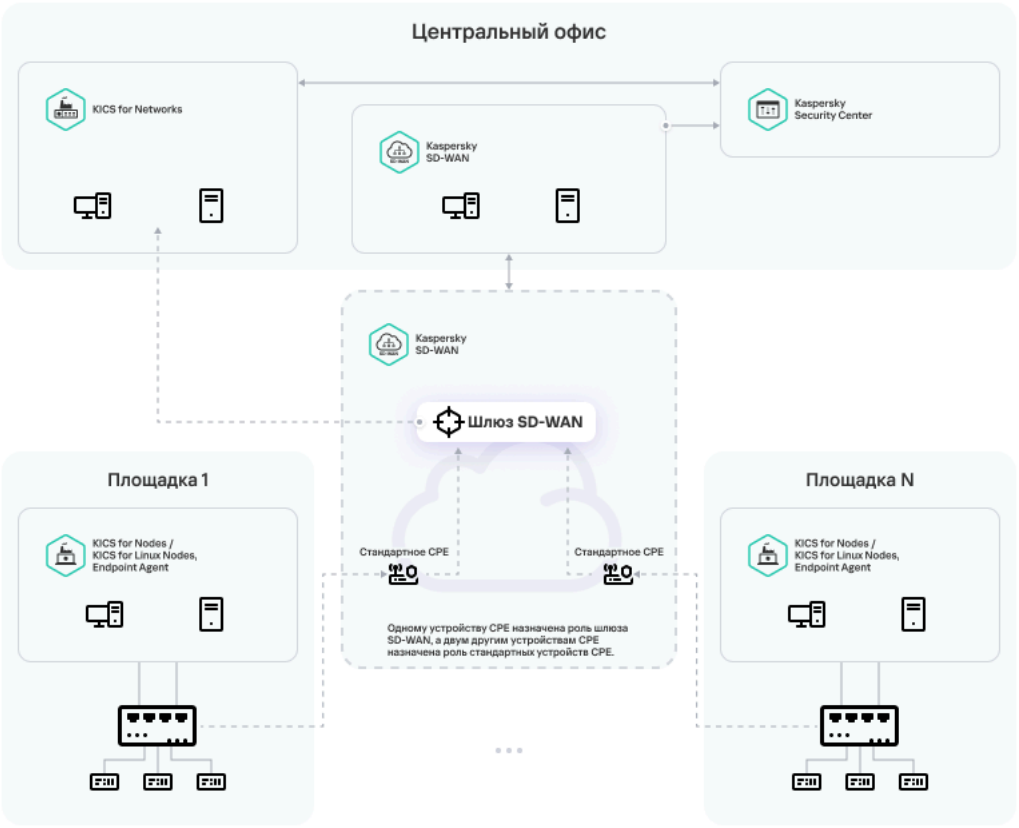
https://support.kaspersky.com/help/KICSforNetworks/4.2/en-US/206298.htm

.

Para mais informações sobre como configurar os componentes do Kaspersky Industrial CyberSecurity for Networks para integração com o Kaspersky SD-WAN, entre em contato com seu Gerente Técnico de Contas (TAM).

Também é possível obter mais informações sobre a integração do Kaspersky SD-WAN com o Kaspersky Industrial CyberSecurity for Networks na seção Apêndices.

A figura abaixo mostra um exemplo de cenário de implementação para o Kaspersky SD-WAN e o Kaspersky Industrial CyberSecurity for Networks. As linhas pontilhadas indicam o caminho do tráfego SPAN. Primeiro, os switches de rede nos locais remotos 1 e N espelham o tráfego para dispositivos CPE com a função de dispositivo CPE padrão. Em seguida, os dispositivos CPE padrão encaminham o tráfego SPAN para o dispositivo CPE com a função de gateway SD-WAN, que, por sua vez, encaminha o tráfego SPAN para o servidor do Kaspersky Industrial CyberSecurity for Networks. Os componentes do Kaspersky SD-WAN e do Kaspersky Industrial CyberSecurity for Networks estão localizados no escritório central da organização.



Exemplo de integração do Kaspersky SD-WAN com o Kaspersky Industrial CyberSecurity for Networks

Contatar o Suporte Técnico

Esta seção descreve as maneiras de obter suporte técnico e os termos sob os quais ele está disponível.

Como obter Suporte Técnico

Se você não encontrar uma solução para o problema na documentação do programa ou em uma das outras fontes de informações sobre o Kaspersky SD-WAN, recomendamos entrar em contato com o Suporte Técnico. A equipe de Suporte Técnico responderá às suas perguntas sobre a instalação e o uso do Kaspersky SD-WAN.

A Kaspersky oferece suporte ao Kaspersky SD-WAN em todo o seu ciclo de vida (consulte a página do ciclo de vida do aplicativo). Antes de entrar em contato com o Serviço de Suporte Técnico, leia as regras de suporte.

É possível entrar em contato com o Suporte Técnico de uma das seguintes maneiras:

- Visitar o site do Suporte Técnico.
- Enviando uma solicitação ao Suporte Técnico pelo portal Kaspersky CompanyAccount.

Suporte Técnico através do Kaspersky CompanyAccount

O Kaspersky CompanyAccount é um portal para organizações que usam aplicativos da Kaspersky. O portal Kaspersky CompanyAccount foi concebido para facilitar a interação entre usuários e os especialistas da Kaspersky por meio de solicitações on-line. O portal Kaspersky CompanyAccount permite monitorar o andamento das solicitações eletrônicas processadas pelos especialistas da Kaspersky e armazenar um histórico de solicitações eletrônicas.

Você pode registrar todos os funcionários da sua empresa com uma única conta no Kaspersky CompanyAccount. Uma única conta permite gerenciar centralmente solicitações de funcionários registrados enviadas para a Kaspersky, além de gerenciar os privilégios desses funcionários através do Kaspersky CompanyAccount.

O portal Kaspersky CompanyAccount está disponível nos seguintes idiomas:

- Inglês
- Espanhol
- Italiano
- Alemão
- Polonês

- Português
- Russo
- Francês
- Japonês

Para saber mais sobre o Kaspersky CompanyAccount, acesse o site do Suporte Técnico.

Fontes de informações sobre a solução

Esta seção lista as fontes de informações sobre a solução.

Você pode selecionar a fonte de informações mais adequada, dependendo do nível de importância e da urgência do problema.

Página do Kaspersky SD-WAN no site da Kaspersky

Na página do Kaspersky SD-WAN, é possível exibir informações gerais sobre o aplicativo, suas funções e recursos.

A página do Kaspersky SD-WAN contém um link para a loja on-line. Lá você pode comprar a solução ou renovar sua licença para usar a solução.

Página do Kaspersky SD-WAN na Base de Conhecimento

A *Base de Conhecimento* é uma seção do site do Suporte Técnico.

Na página do Kaspersky SD-WAN na Base de Conhecimento, é possível ler artigos que fornecem informações úteis, recomendações e respostas às perguntas frequentes sobre como comprar, instalar e usar a solução.

Os artigos da Base de Conhecimento podem fornecer respostas a perguntas relacionadas ao Kaspersky SD-WAN e a outros aplicativos da Kaspersky. Os artigos da Base de Conhecimento também podem incluir notícias do Suporte Técnico.

Discutir questões sobre os aplicativos da Kaspersky no fórum

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky e outros usuários em nosso Fórum.

No Fórum, você pode ver tópicos publicados, adicionar comentários e criar novos tópicos.

Apêndices

Obtenha informações adicionais sobre o Kaspersky SD-WAN nos seguintes guias:

- Guia de implementação do Kaspersky SD-WAN em plataforma de teste para um ambiente VMware, parte 1.
- Guia de implementação do Kaspersky SD-WAN em plataforma de teste para um ambiente VMware, parte 2.
- Manual do usuário KESR Modelo 1.
- Manual do usuário KESR Modelo 2 (versão 1).
- Manual do usuário KESR Modelo 2 (versão 2).
- Manual do usuário KESR Modelo 3.
- Manual do usuário KESR Modelo 4 (versão 1).
- Manual do usuário KESR Modelo 4 (versão 2).
- Manual do usuário KESR Modelo 5 (versão 1).
- Manual do usuário KESR Modelo 5 (versão 2).
- Encaminhar tráfego SPAN através da malha SD-WAN para teste de cenários KICS.

Glossário

Controlador

Gerencia de forma centralizada a rede overlay:

- Cria a topologia da rede.
- Cria serviços de transporte.
- Gerencia dispositivos CPE usando o protocolo OpenFlow.
- Equilibra o tráfego entre links.
- Monitora links e muda o tráfego automaticamente para um link de backup se o link principal falhar.

Para implementar o controlador, é necessário implementar a função de rede física do controlador, contida no arquivo de instalação. O controlador é gerenciado pelo orquestrador.

CPE universal (uCPE)

CPEs com suporte adicional para implementação de Funções de rede virtual. O dispositivo uCPE deve ter recursos de hardware suficientes para fornecer funções de rede virtual sem envolver o data center ou a nuvem.

Equipamento nas instalações do cliente (CPE)

Equipamento de telecomunicações, incluindo máquinas virtuais, localizado nas instalações do cliente. Usados para conectar o local do cliente à rede SD-WAN, estabelecer links e transferir tráfego entre os locais do cliente. O tráfego pode ser enviado a um data center para fornecer funções de rede, como protocolos de roteamento, prevenção de intrusão ou proteção antivírus.

Estratégia de transporte

Um mecanismo de encapsulamento do serviço de transporte que inclui o algoritmo para adicionar uma stack de tags de cabeçalho de pacote de tráfego e o tipo dessas tags. O Kaspersky SD-WAN tem suporte temporário uma estratégia de transporte, **Transporte genérico de troca de VNI**.

Função de rede física (PNF)

Funções de rede implementadas como hardwares especializados ou entidades virtuais criadas usando ambientes de virtualização de terceiros. O orquestrador não gerencia o ciclo de vida das funções de rede física.

Função de rede virtual (VNF)

As funções de rede implementadas como máquinas virtuais em plataformas de computador Commercial Off The Shelf (COTS). O ciclo de vida das funções de rede virtual é gerenciado por um orquestrador. Para implementar funções de rede virtual, é necessário usar a plataforma em nuvem OpenStack.

Gateway SD-WAN

Dispositivo CPE com a função de gateway SD-WAN. Os gateways SD-WAN estabelecem links com todos os dispositivos na rede, incluindo outros gateways SD-WAN, fornecendo assim a conexão entre todos os dispositivos CPE e o controlador. É possível instalar diversos gateways SD-WAN para tolerância a falhas.

Gerenciador de funções de rede virtual (VNFM)

Gerencia o ciclo de vida das funções de rede virtual usando SSH, manuais do Ansible, scripts e atributos Cloud-init.

Gerenciador de infraestrutura virtual (VIM)

Gerencia recursos computacionais, de rede e de armazenamento na infraestrutura de NFV. Serve para conectar funções de rede com links virtuais, sub-redes e portas.

Pode ser implementado no data center ou num dispositivo uCPE. A implementação do VIM no data center implica o gerenciamento centralizado do ciclo de vida do VNF, enquanto um VIM implementado num dispositivo uCPE permite entregar VNFs a locais remotos e gerenciá-los localmente. O VIM implementado deve ser adicionado à interface da Web do orquestrador.

A plataforma de nuvem OpenStack é usada como o VIM.

Instância SD-WAN

Uma solução Kaspersky SD-WAN implementada para um dos locatários de sua organização. É uma entidade isolada e tem seus próprios serviços de rede, dispositivos CPE e parâmetros de qualidade de serviço.

Locatário

Uma entidade lógica dentro da qual uma instância de SD-WAN individual é implementada. Componentes da solução, como componentes de serviço de rede, usuários e dispositivos CPE, são atribuídos a um locatário e, posteriormente, os administradores de locatários podem gerenciar os componentes atribuídos. Por exemplo, é possível criar um locatário separado para um cliente de sua organização.

Open vSwitch (OVS)

Tipo de switch de software que serve como base do firmware do dispositivo CPE. Essa implementação usa o processamento de pacotes no nível do kernel e é adequada para a maioria dos dispositivos.

Orquestrador

Controla a infraestrutura da solução, funciona como orquestrador de NFV (NFVO) e gerencia serviços de rede e gerenciadores de VNF distribuídos (VNFMs). É possível gerenciar o orquestrador por meio da interface da Web ou da API REST ao usar sistemas externos northbound.

Pacote da PNF

Um pacote, no formato TAR ou ZIP, que contém os dados necessários para implementar e gerenciar a PNF.

Pacote da VNF

Um pacote, no formato TAR ou ZIP, que contém os dados necessários para implementar e gerenciar uma VNF.

Plano de controle

A parte da rede responsável por controlar a transmissão de pacotes de tráfego por meio de dispositivos CPE. Executa funções como descoberta de rede, cálculo de rota, priorização de tráfego e aplicação de políticas de segurança. O plano de controle permite o gerenciamento centralizado da rede ao fornecer uma visão completa de todas as operações executadas. Consiste em um orquestrador e um controlador.

Plano de dados

A parte da rede que processa e transmite o tráfego entre diferentes locais e dispositivos. O plano de dados usa protocolos de rede e algoritmos para rotear e fornecer tráfego pela rede com eficiência. Consiste em dispositivos CPE.

Rede de longa distância definida por software (SD-WAN)

Abordagem para a construção de redes definidas por software usando uma rede global de computadores. As redes SD-WAN permitem conectar redes locais e usuários em locais geograficamente dispersos.

Rede definida por software (SDN)

Tecnologia para construir redes de comunicação em que o plano de controle é separado do plano de dados e implementado em softwares usando um controlador SDN centralizado.

Segurança de portas

Essa função melhora a segurança da rede no nível das portas Ethernet dos switches e evita o acesso não autorizado à rede ao limitar o número de endereços MAC que podem ser associados a uma única porta física. Quando ativada, apenas dispositivos confiáveis com endereços MAC predefinidos podem estabelecer conexão com a rede.

Switch Operating System (SWOS)

Tipo de switch de software que serve como base do firmware do dispositivo CPE. É uma implementação alternativa com processamento de pacotes baseado em DPDK. Pode oferecer maior desempenho graças ao processamento de pacotes com bypass do kernel.

Unidade de implementação virtual (VDU)

Uma máquina virtual que atua como host VNF e agrega recursos de computação virtual, como CPU e memória, necessários para executar o software VNF, além de conter determinadas implementações da função de rede, como algoritmos de roteamento ou lógica de balanceamento de carga.

Vários VDUs podem ser combinados num único VNF para fornecer escalabilidade e/ou alta disponibilidade. Os VDUs podem estar distribuídos em diversos servidores físicos; ainda será possível gerenciá-los como um único VNF. Os VDUs interagem entre si e com outros VNFs para executar suas funções dentro de um serviço de rede.

Informação sobre código de terceiros

Informações sobre códigos de terceiros podem ser encontradas no arquivo legal_notices.txt na pasta de instalação do aplicativo.

Avisos de marca registrada

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Active Directory é uma marca comercial do grupo de empresas Microsoft.

Ansible, CentOS, Red Hat são marcas comerciais ou registradas nos Estados Unidos e em outros países da Red Hat, Inc. ou de suas subsidiárias.

Arm é uma marca registrada da Arm Limited (ou de suas subsidiárias) nos EUA e/ou em outros países.

Atom, Celeron, Intel e Xeon são marcas comerciais da Intel Corporation ou de suas subsidiárias.

Debian é uma marca registrada de software na Public Interest, Inc.

Docker e o logotipo Docker são marcas comerciais ou marcas registradas da Docker, Inc. nos EUA e/ou em outros países. A Docker, Inc. e outras partes podem ter direitos sobre marcas registradas descritas com outros termos usados neste documento.

Firefox é uma marca registrada da Mozilla Foundation nos EUA e em outros países.

Android é uma marca comercial da Google LLC.

IBM é uma marca comercial da International Business Machines Corporation, registrada em muitas jurisdições em todo o mundo.

Intel e Xeon são marcas comerciais da Intel Corporation ou de suas subsidiárias.

Kraftway é uma marca registrada da AO Kraftway Corporation PLC.

Linux, LTS são marcas registradas da Linus Torvalds nos EUA e em outros países.

Microsoft Edge e Windows são marcas registradas do grupo de empresas Microsoft.

MIPS é uma marca comercial ou marca registrada da MIPS Technologies nos EUA e em outros países.

OpenStack é uma marca registrada da OpenStack Foundation nos EUA e em outros países.

OpenStreetMap é uma marca registrada da OpenStreetMap Foundation. Este produto não é afiliado com a OpenStreetMap Foundation ou endossado por ela.

Python é uma marca comercial ou marca registrada da Python Software Foundation.

Safari é uma marca registrada da Apple Inc.

SUSE é uma marca comercial da SUSE LLC registrada nos Estados Unidos e em outros lugares.

Ubuntu é uma marca registrada da Canonical Ltd.

VMware é uma marca registrada e/ou marca comercial da VMware, Inc. nos Estados Unidos e em outros países.

Zabbix é uma marca registrada da Zabbix SIA.