kaspersky

Kaspersky SD-WAN

© 2025 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky SD-WAN

О Kaspersky SD-WAN

- Комплект поставки
- Аппаратные и программные требования
- Обеспечение безопасности

Что нового

Архитектура решения

Развертывание Kaspersky SD-WAN

- Резервирование компонентов решения
- Настройка балансировки нагрузки между экземплярами оркестратора
- Об архиве установки
- О режимах выполнения действий attended, unattended и partially attended
- Подготовка устройства администратора
- Работа с паролями
  - Ручная генерация паролей
  - Изменение паролей
- Настройка конфигурационного файла
- Изменение графических элементов веб-интерфейса оркестратора
- Замена вышедшего из строя узла контроллера
- Обновление Kaspersky SD-WAN
- Удаление Kaspersky SD-WAN

Вход и выход из веб-интерфейса оркестратора

Лицензирование Kaspersky SD-WAN

- О Лицензионном соглашении
- О предоставлении данных

Интерфейс решения

- Установка и сброс страницы по умолчанию
- Переключение между светлым и темным режимом веб-интерфейса оркестратора
- Изменение языка веб-интерфейса оркестратора
- Работа с таблицами компонентов решения

Переход к API оркестратора

Управление инфраструктурой Kaspersky SD-WAN

- Работа с доменами
  - Создание домена
  - Изменение домена
  - Удаление домена
- Работа с центрами обработки данных
  - Добавление центра обработки данных
  - Изменение центра обработки данных
  - Перемещение центра обработки данных в другой домен
  - Удаление центра обработки данных
- Работа с подсетями управления
  - Создание подсети управления

- Изменение подсети управления
- Удаление подсети управления
- Работа с контроллерами
  - Изменение контроллера
  - Перезагрузка контроллера
  - Восстановление параметров контроллера
  - Включение и выключение режима обслуживания на контроллере
  - Удаление контроллера
  - Работа со свойствами контроллера
    - Описание изменяемых свойств контроллера
    - Изменение свойства контроллера
    - Удаление запланированных значений свойств контроллера
    - Сброс свойств контроллера до значений по умолчанию
  - Просмотр информации об узлах контроллера
- Работа с VIM
  - Настройка VIM, развернутого в центре обработки данных
  - Настройка VIM, развернутого на устройстве uCPE
  - Изменение VIM, развернутого в центре обработки данных
  - Просмотр вычислительных ресурсов, используемых VIM
  - Удаление VIM

Управление пользователями и их правами доступа

- Работа с правами доступа
  - Создание права доступа
  - Изменение права доступа
  - Клонирование права доступа
  - Удаление права доступа
- Работа с LDAP-подключениями
  - Создание LDAP-подключения
  - Изменение LDAP-подключения
  - Изменение пароля LDAP-подключения
  - Удаление LDAP-подключения
- Работа с пользователями
  - Создание пользователя
  - Разблокировка и блокировка пользователя
  - Изменение пользователя
  - Изменение пароля локального пользователя
  - Повторная двухфакторная аутентификация пользователя
  - Удаление пользователя
- Работа с группами LDAP-пользователей
  - Создание группы LDAP-пользователей
  - Изменение группы LDAP-пользователей
  - Удаление группы LDAP-пользователей
- Включение и выключение двухфакторной аутентификации для всех пользователей
- Работа с запросами на подтверждение
- Работа с пользовательскими сеансами

Мультитенантность

- Сценарий: развертывание экземпляра SD-WAN для тенанта

- Работа с тенантами
  - Создание тенанта
  - Назначение тенанту пользователя
  - Назначение тенанту группы LDAP-пользователей
  - Назначение тенанту вычислительных ресурсов
  - Назначение тенанту компонентов сетевого сервиса
  - Назначение тенанту VIM
  - Вход на портал самообслуживания тенанта
  - Изменение тенанта
  - Удаление тенанта
- Работа с шаблонами экземпляра SD-WAN
  - Создание шаблона экземпляра SD-WAN
  - Назначение шаблона экземпляра SD-WAN по умолчанию
  - Выбор количества узлов контроллера экземпляра SD-WAN
  - Добавление тенанта в шаблон экземпляра SD-WAN
  - Удаление тенанта из шаблона экземпляра SD-WAN
  - Удаление шаблона экземпляра SD-WAN
- Работа с экземплярами SD-WAN
  - Настройка узлов контроллера экземпляра SD-WAN
  - Просмотр использования экземпляра SD-WAN
  - Просмотр топологии экземпляра SD-WAN
  - Добавление тенанта в экземпляр SD-WAN
  - Удаление тенанта из экземпляра SD-WAN
  - Удаление экземпляра SD-WAN
- Работа с пулами экземпляров SD-WAN
  - Создание пула экземпляров SD-WAN
  - Добавление экземпляра SD-WAN в пул экземпляров SD-WAN
  - Удаление экземпляра SD-WAN из пула экземпляров SD-WAN
  - Удаление пула экземпляров SD-WAN

Управление устройствами CPE

- О взаимодействии между устройством CPE и оркестратором
- О взаимодействии между устройством CPE и контроллером
- Учетные данные по умолчанию устройств CPE модели KESR
- Проверка целостности
- Регистрация устройств CPE
  - Сценарий: регистрация устройства CPE с использованием технологии Zero Touch Provisioning
  - Сценарий: развертывание на платформе виртуализации VMware и регистрация устройства vCPE с использованием технологии Zero Touch Provisioning
  - Сценарий: повторная регистрация устройства CPE
  - Возобновление регистрации устройства CPE при возникновении ошибки
- Работа с шаблонами CPE
  - Создание шаблона CPE
  - Импорт шаблона CPE
  - Клонирование шаблона CPE
  - Экспорт параметров подключения к оркестратору и контроллеру, и интерфейсов SD-WAN из шаблона CPE
  - Экспорт сетевых интерфейсов из шаблона CPE
  - Просмотр использования шаблона CPE

- Удаление шаблона CPE
- Работа с устройствами CPE
  - Добавление устройств CPE
  - Массовый импорт устройств CPE из файла CSV
  - Генерация веб-адреса с базовыми параметрами устройства CPE
  - Регистрация устройства CPE вручную
  - Отмена регистрации устройства CPE
  - Указание адреса устройства CPE
  - Включение и выключение устройства CPE
  - Перезагрузка устройства CPE
  - Выключение питания устройства CPE
  - Подключение к консоли устройства CPE
  - Просмотр пароля устройства CPE
  - Экспорт параметров подключения к оркестратору и контроллеру и интерфейсов SD-WAN из устройства CPE
  - Экспорт сетевых интерфейсов из устройства CPE
  - Изменение идентификатора DPID устройства CPE
  - Изменение параметров устройств CPE
  - Удаление устройств CPE
- Двухфакторная аутентификация устройства CPE
- Работа с сертификатами
  - Загрузка сертификата в веб-интерфейс оркестратора
  - Ручная установка сертификатов на устройствах CPE
  - Сценарий: установка сертификатов на устройстве CPE с версией прошивки 23.07
  - Экспорт сертификата
  - Удаление сертификатов
- Работа со справочниками APN
  - Создание справочника APN
- Просмотр и сброс сессий на устройствах CPE
- Автоматическое удаление и выключение устройств CPE
- Группировка устройств CPE с помощью тегов
  - Назначение тега устройствам CPE
  - Удаление тега устройств CPE
- Настройка журналов на устройствах CPE
- Работа с модемами
- Обновление прошивки
  - Обновление прошивки на устройстве CPE вручную
  - Загрузка прошивки в веб-интерфейс оркестратора
  - Запланированное обновление прошивки на выбранных устройствах CPE
  - Запланированное обновление прошивки на устройствах CPE с указанными тегами
  - Восстановление прошивки устройства CPE модели KESR-M1
  - Восстановление прошивки устройства CPE модели KESR-M2–5
  - Соответствие моделей устройств CPE версиям прошивок
  - Удаление прошивки
- Дополнительная настройка устройств CPE с помощью скриптов
  - Добавление скрипта на устройства CPE
  - Запуск скриптов вручную на устройствах CPE
  - Запланированный запуск скриптов на устройствах CPE

- Изменение скрипта на устройствах CPE
- Удаление скрипта на устройствах CPE

Настройка параметров DNS на устройствах CPE
- Включение DNS на сетевых интерфейсах
- Работа с правилами условной переадресации DNS
  - Создание правил условной переадресации
  - Изменение правил условной переадресации
  - Удаление правил условной переадресации

Настройка подключения устройства CPE к оркестратору и контроллеру

Настройка параметров подключения к устройству CPE через системную консоль

Работа с сетевыми интерфейсами
- Создание сетевых интерфейсов
  - Создание сетевого интерфейса с автоматическим назначением IP-адреса по протоколу DHCP
  - Создание сетевого интерфейса со статическим IPv4-адресом
  - Создание сетевого интерфейса со статическим IPv6-адресом
  - Создание сетевого интерфейса для подключения к LTE-сети
  - Создание сетевого интерфейса для подключения к PPPoE-серверу
  - Создание сетевого интерфейса без IP-адреса
- Изменение сетевого интерфейса
- Выключение и включение сетевого интерфейса
- Отмена применения параметров сетевых интерфейсов к устройству CPE
- Удаление сетевого интерфейса
- Защита от IP-спуфинга с помощью uRPF

Работа с интерфейсами SD-WAN
- О передаче контроллеру информации об интерфейсах SD-WAN с типом WAN
- Фрагментация пакетов
- Очереди трафика на интерфейсах SD-WAN
- Создание интерфейса SD-WAN с типом WAN
- Изменение интерфейса SD-WAN
- Выключение и включение интерфейса SD-WAN
- Удаление интерфейса SD-WAN с типом WAN

Работа с сервисными интерфейсами
- Создание сервисного интерфейса
- Создание ACL-интерфейса
- Просмотр использования сервисного интерфейса и ACL-интерфейса
- Удаление сервисного интерфейса и ACL-интерфейса

Работа с группами OpenFlow-портов
- Создание группы OpenFlow-портов
- Изменение группы OpenFlow-портов
- Удаление группы OpenFlow-портов

Настройка UNI для подключения устройств CPE к сетевым сервисам
- Работа с шаблонами UNI
  - Создание шаблона UNI
  - Удаление шаблона UNI
- Работа с UNI
  - Создание UNI
  - Просмотр использования UNI

- Изменение UNI
- Удаление UNI

Добавление статического маршрута

- Таблица соответствия административных расстояний для протоколов маршрутизации

Фильтрация маршрутов и пакетов трафика

- Работа со списками управления доступом (ACLs)
  - Создание списка управления доступом
  - Изменение списка управления доступом
  - Удаление списка управления доступом
- Работа со списками префиксов (prefix lists)
  - Создание списка префиксов
  - Изменение списка префиксов
  - Удаление списка префиксов
- Работа со списками community
  - Создание списка community
  - Изменение списка community
  - Удаление списка community
- Работа с картами маршрутизации (route maps)
  - Создание карты маршрутизации
  - Изменение карты маршрутизации
  - Удаление карты маршрутизации

Маршрутизация на основе политик (PBR)

- Работа с IP-правилами маршрутизации
  - Создание IP-правила
  - Изменение IP-правила
  - Удаление IP-правила

Обмен маршрутами по протоколу BGP

- Настройка основных параметров BGP
- Работа с BGP-соседями (BGP peers)
  - Создание BGP-соседа
  - Изменение BGP-соседа
  - Удаление BGP-соседа
- Работа с группами BGP-соседей (BGP peer groups)
  - Создание группы BGP-соседей
  - Изменение группы BGP-соседей
  - Удаление группы BGP-соседей
- Настройка параметров обмена маршрутами между VRF (Inter-VFR Route Leaking)

Обмен маршрутами по протоколу OSPF

- Настройка основных параметров OSPF
- Работа с OSPF-областями
  - Создание OSPF-области
  - Изменение OSPF-области
  - Удаление OSPF-области
- Работа с OSPF-интерфейсами
  - Создание OSPF-интерфейса
  - Изменение OSPF-интерфейса
  - Удаление OSPF-интерфейса

Обнаружение ошибок маршрутизации с помощью протокола BFD
Включение и выключение протокола BFD
Создание BFD-соседа
Изменение BFD-соседа
Удаление BFD-соседа
Обеспечение высокой доступности с помощью протокола VRRP
Включение и выключение протокола VRRP
Работа с экземплярами VRRP
Создание экземпляра VRRP
Изменение экземпляра VRRP
Удаление экземпляра VRRP
Работа с группами экземпляров VRRP
Создание группы экземпляров VRRP
Изменение группы экземпляров VRRP
Удаление группы экземпляров VRRP
Передача multicast-трафика с помощью протоколов PIM и IGMP
Настройка основных параметров PIM
Работа с multicast-интерфейсами
Создание multicast-интерфейса
Изменение multicast-интерфейса
Удаление multicast-интерфейса
Работа с виртуальными таблицами маршрутизации (VRF)
Настройка параметров ядра, связанных с виртуальными таблицами маршрутизации
Создание виртуальной таблицы маршрутизации
Изменение виртуальной таблицы маршрутизации
Удаление виртуальной таблицы маршрутизации
Отслеживание информации о пакетах трафика с помощью протокола NetFlow
Работа с шаблонами NetFlow
Создание шаблона NetFlow
Выбор назначенного шаблона NetFlow
Импорт шаблона NetFlow
Клонирование шаблона NetFlow
Просмотр использования шаблона NetFlow
Удаление шаблона NetFlow
Настройка основных параметров NetFlow
Изменение шаблона NetFlow устройства CPE
Диагностика устройства CPE
Запрос диагностической информации
Использование режима отладки для протоколов динамической маршрутизации на устройствах CPE
Указание NTP-серверов на устройствах CPE
Включение интерактивного режима
Запуск утилиты ping
Запуск утилиты traceroute
Запуск утилиты tcpdump
Запуск утилиты iperf
Запуск утилиты sweep
Запуск утилиты OpenFlow dump

- Сброс сессий BGP/OSPF
- Работа с отчетами
  - Скачивание отчета
  - Удаление отчета
- Выполнение задач на устройствах CPE
  - Создание задачи
  - Выполнение задачи вручную
  - Удаление задачи
- Проверки CPE
  - Проверка целостности
    - Запуск проверки целостности по требованию
    - Запуск проверки целостности по расписанию
  - Самотестирование межсетевого экрана
    - Запуск самотестирования межсетевого экрана по требованию
    - Запуск самотестирования межсетевого экрана по расписанию
  - Блокировка трафика при ошибках самотестирования и проверки целостности
- Аудит событий безопасности
  - Настройка регистрации событий безопасности для аудита
  - Перечень событий безопасности, регистрируемых на оркестраторе и устройствах CPE
- Диапазоны IP-адресов и подсетей для устройств CPE
  - Работа с диапазонами IP-адресов
    - Создание диапазона IP-адресов
    - Изменение диапазона IP-адресов
    - Просмотр использования диапазона IP-адресов
    - Удаление диапазонов IP-адресов
  - Работа с диапазонами подсетей
    - Создание диапазона подсетей
    - Изменение диапазона подсетей
    - Просмотр использования диапазона подсетей
    - Удаление диапазонов подсетей
- Управление межсетевым экраном
  - Работа с зонами межсетевого экрана
    - Создание зоны межсетевого экрана
    - Клонирование общей зоны межсетевого экрана
    - Просмотр использования общей зоны межсетевого экрана
    - Изменение зоны межсетевого экрана
    - Удаление зоны межсетевого экрана
  - Работа с шаблонами межсетевого экрана
    - Создание шаблона межсетевого экрана
    - Выбор назначенного шаблона межсетевого экрана
    - Импорт шаблона межсетевого экрана
    - Клонирование шаблона межсетевого экрана
    - Просмотр использования шаблона межсетевого экрана
    - Удаление шаблона межсетевого экрана
  - Настройка основных параметров межсетевого экрана
  - Настройка маркировки DPI
  - Работа с правилами межсетевого экрана

- Создание правила межсетевого экрана
- Настройка порядка применения правил межсетевого экрана
- Включение и выключение правила межсетевого экрана
- Изменение правила межсетевого экрана
- Удаление правила межсетевого экрана
- Работа с расширенными правилами межсетевого экрана
  - Дополнительные критерии совпадения для расширенных правил
    - Фрагментированный пакет
    - Совпадение по метке
    - TOS
    - Совпадение по строке
    - Совпадение по недавним
    - Недопустимые TCP-флаги
    - Ограничение частоты
    - Мобильный код
    - Совпадение по командам протоколов прикладного уровня
  - Создание расширенного правила
  - Включение и выключение расширенных правил
  - Изменение расширенного правила
  - Удаление расширенного правила
  - Клонирование расширенного правила
  - Сценарий: скрытие устройства CPE на пути прохождения трафика с помощью расширенных правил межсетевого экрана
- Работа с наборами IP
  - Создание набора IP
  - Выключение и включение набора IP
  - Изменение набора IP
  - Удаление набора IP
- Работа с DNAT-правилами
  - Создание DNAT-правила
  - Настройка порядка применения DNAT-правил
  - Выключение и включение DNAT-правила
  - Изменение DNAT-правила
  - Удаление DNAT-правила
- Работа с SNAT-правилами
  - Создание SNAT-правила
  - Настройка порядка применения SNAT-правил
  - Выключение и включение SNAT-правила
  - Изменение SNAT-правила
  - Удаление SNAT-правила
- Работа с передачами
  - Создание передачи
  - Удаление передачи
- Изменение шаблона межсетевого экрана устройства CPE

Интеграция с внешними средствами защиты информации

Управление сетевыми сервисами и виртуализация сетевых функций

- Работа с шаблонами сетевых сервисов

- Создание шаблона сетевого сервиса
- Изменение шаблона сетевого сервиса
- Удаление шаблона сетевого сервиса

Работа с сетевыми сервисами

- Создание сетевого сервиса
- Изменение сетевого сервиса
- Развертывание сетевого сервиса
- Проверка консистентности сетевого сервиса
- Повторное развертывание сетевого сервиса
- Выключение и включение автоматического восстановления сетевого сервиса
- Просмотр журнала работы сетевого сервиса
- Удаление сетевого сервиса

Сценарий: развертывание виртуальной сетевой функции

Сценарий: развертывание физической сетевой функции

Работа с пакетами VNF и PNF

- Настройка VNF-дескриптора
- Настройка PNF-дескриптора
- Защита пакетов VNF и PNF от подмены и изменения
- Загрузка пакета VNF или PNF в веб-интерфейс оркестратора

Указание краткого описания общего сетевого сервиса

Работа с виртуальными сетевыми функциями

- Выбор варианта развертывания виртуальной сетевой функции
- Настройка внешних точек подключения виртуальной сетевой функции
- Настройка основных параметров виртуальной сетевой функции
- Размещение виртуальной сетевой функции в центре обработки данных и на устройстве uCPE
- Остановка и запуск виртуальной сетевой функции или входящей в ее состав VDU
- Пауза и снятие с паузы виртуальной сетевой функции или входящей в ее состав VDU
- Перевод виртуальной сетевой функции или входящей в ее состав VDU в состояние сна и активное состояние
- Программная перезагрузка виртуальной сетевой функции или входящей в ее состав VDU
- Аппаратная перезагрузка виртуальной сетевой функции или входящей в ее состав VDU
- Повторное развертывание виртуальной сетевой функции или входящей в ее состав VDU
- Автоматическое восстановление виртуальной сетевой функции или входящей в ее состав VDU
- Работа с снимками состояния VDU
  - Создание снимка состояния VDU
  - Восстановление параметров VDU с помощью снимка состояния
  - Изменение снимка состояния VDU
  - Удаление снимка состояния VDU

Работа с физическими сетевыми функциями

- Выбор варианта развертывания физической сетевой функции
- Настройка основных параметров физической сетевой функции

Настройка P2P-сервиса

Настройка P2M-сервиса

Настройка M2M-сервиса

Настройка общей сети (OS 2 SHARED)

Настройка виртуального маршрутизатора (OS vRouter)

Настройка VLAN

Настройка VXLAN

- Настройка плоской сети
- Настройка UNI

Мониторинг компонентов решения
- Указание сервера Zabbix
- Указание сервера Zabbix-прокси
- Настройка мониторинга устройств CPE
- Просмотр результатов мониторинга
- Просмотр проблем
- Просмотр состояния решения и его компонентов
- Просмотр журналов
- Просмотр и удаление сервисных запросов
- Отправка уведомлений об устройствах CPE пользователям
  - Указание SMTP-сервера
  - Настройка отправки уведомлений
- Выбор уровня детализации журналов Docker-контейнеров
- Мониторинг устройств CPE, VNF и PNF с помощью протокола SNMP
  - Настройка подключения SNMP-менеджера к SNMP-агентам
  - Создание уведомления-ловушки
  - Изменение уведомления-ловушки
  - Удаление уведомления-ловушки
- Мониторинг соединения

Построение сети SD-WAN между устройствами CPE
- О топологии Hub-and-Spoke
- О топологиях Full-Mesh и Partial-Mesh
- Назначение роли устройству CPE
- Назначение топологического тега устройству CPE
- Настройка путей
- Работа с соединениями
  - Просмотр статистики соединения
  - Автоматическое изменение стоимости соединения в зависимости от максимальной скорости интерфейса
  - Указание стоимости соединения
  - Включение функции Dampening
  - Включение функции Forward Error Correction
  - Определение значения MTU
  - Шифрование трафика
    - Включение шифрования трафика на устройстве CPE
    - Включение шифрования трафика на соединении
  - Функция Connectivity Fault Management (CFM)
    - Включение функции CFM на устройстве CPE
    - Включение функции CFM на соединении
- Работа с сегментами
  - Создание пути Manual-TE
  - Изменение пути Manual-TE
  - Удаление пути Manual-TE

Качество обслуживания (QoS)
- Механизмы качества обслуживания
- Маркировка и перемаркировка трафика

- Работа с классами трафика
- Работа с классификаторами трафика
  - Создание классификатора трафика
  - Изменение классификатора трафика
  - Удаление классификатора трафика
- Работа с правилами качества обслуживания
  - Создание правила качества обслуживания
  - Изменение правила качества обслуживания
  - Удаление правила качества обслуживания
- Работа с ограничениями Manual-TE
  - Создание ограничения Manual-TE
  - Изменение ограничения Manual-TE
  - Удаление ограничения Manual-TE
- Работа с пороговыми ограничениями
  - Создание порогового ограничения
  - Изменение порогового ограничения
  - Удаление порогового ограничения
- Работа с правилами классификации трафика
  - Создание правила классификации трафика
  - Изменение правила классификации трафика
  - Удаление правила классификации трафика
- Работа с фильтрами трафика
  - Создание фильтра трафика
  - Изменение фильтра трафика
  - Удаление фильтра трафика

Передача трафика между устройствами CPE и клиентскими устройствами с помощью транспортных сервисов

- Дублирование пакетов трафика
- Сценарий: направление трафика приложения в транспортный сервис
- Сценарий: обеспечение L2-связности между устройствами CPE
- Сценарий: управление трафиком приложений в соответствии с заданным SLA
- Работа с транспортными сервисами Point-to-Point (P2P)
  - Создание P2P-сервиса
  - Просмотр статистики работы P2P-сервиса
  - Просмотр и настройка отображения топологии P2P-сервиса
  - Изменение P2P-сервиса
  - Перезагрузка P2P-сервиса
  - Удаление P2P-сервиса
- Работа с транспортными сервисами Point-to-Multipoint (P2M)
  - Создание P2M-сервиса
  - Просмотр статистики работы P2M-сервиса
  - Просмотр MAC-таблицы P2M-сервиса
  - Просмотр и настройка отображения топологии P2M-сервиса
  - Изменение P2M-сервиса
  - Перезагрузка P2M-сервиса
  - Удаление P2M-сервиса
- Работа с транспортными сервисами Multipoint-to-Multipoint (M2M)
  - Создание M2M-сервиса

Просмотр статистики работы M2M-сервиса
Просмотр MAC-таблицы M2M-сервиса
Просмотр и настройка отображения топологии M2M-сервиса
Изменение M2M-сервиса
Перезагрузка M2M-сервиса
Удаление M2M-сервиса
Работа с транспортными сервисами IP multicast
Создание IP multicast-сервиса
Просмотр статистики работы IP multicast-сервиса
Изменение IP multicast-сервиса
Удаление IP multicast-сервиса
Работа с транспортными сервисами L3 VPN
Создание L3 VPN-сервиса
Работа с ARP-таблицей L3 VPN-сервиса
Создание статической записи в ARP-таблице L3 VPN-сервиса
Изменение статической записи в ARP-таблице L3 VPN-сервиса
Удаление статической записи в ARP-таблице L3 VPN-сервиса
Просмотр таблицы маршрутизации L3 VPN-сервиса
Изменение L3 VPN-сервиса
Перезагрузка L3 VPN-сервиса
Удаление L3 VPN-сервиса
Работа с транспортными сервисами в шаблоне экземпляра SD-WAN
Создание P2M-сервиса или M2M-сервиса в шаблоне экземпляра SD-WAN
Создание L3 VPN-сервиса в шаблоне экземпляра SD-WAN
Изменение транспортного сервиса в шаблоне экземпляра SD-WAN
Удаление транспортного сервиса в шаблоне экземпляра SD-WAN
Работа с транспортными сервисами в шаблоне CPE
Добавление транспортного сервиса в шаблон CPE
Изменение транспортного сервиса в шаблоне CPE
Удаление в транспортного сервиса в шаблоне CPE
Зеркалирование и перенаправление трафика между устройствами CPE
Работа с точками назначения трафика
Создание точки назначения трафика
Удаление точки назначения трафика
Работа с TAP-сервисами
Создание TAP-сервиса
Просмотр статистики работы TAP-сервиса
Изменение TAP-сервиса
Удаление TAP-сервиса
Интеграция с Kaspersky Unified Monitoring and Analysis Platform
Установка KUMA
Сценарий: настройка KUMA
Настройка хранилища в KUMA
Создание и настройка нормализатора в KUMA для syslog-событий
Настройка коррелятора и правил корреляции в KUMA
Справочная таблица для создания правил корреляции KUMA
Настройка коллектора для syslog-событий в KUMA

Настройка почтовой службы в KUMA
Настройка правил уведомления в KUMA
Примеры настройки для поиска по ключевым событиям в KUMA
Интеграция с Kaspersky CyberSecurity for Networks
Обращение в Службу технической поддержки
Способы получения технической поддержки
Техническая поддержка через Kaspersky CompanyAccount
Источники информации о решении
Приложения
Глоссарий
Customer Premise Equipment (CPE)
Open vSwitch (OVS)
Physical Network Function (PNF)
Port security
Software-Defined Networking (SDN)
Software-Defined Wide Area Network (SD-WAN)
Switch Operating System (SWOS)
Universal CPE (uCPE)
Virtual Deployment Unit (VDU)
Virtual Infrastructure Manager (VIM)
Virtual Network Function (VNF)
Virtual Network Function Manager (VNFM)
Контроллер
Оркестратор
Пакет PNF
Пакет VNF
Плоскость передачи данных
Плоскость управления сетью
Тенант
Транспортная стратегия
Шлюз SD-WAN
Экземпляр SD-WAN
Информация о стороннем коде
Уведомления о товарных знаках

Справка Kaspersky SD-WAN

Новые функции

Что нового в каждой версии Kaspersky SD-WAN

Аппаратные и программные требования

Проверьте требования к аппаратным и программным ресурсам

Начало работы

- Развертывание Kaspersky SD-WAN
- Управление инфраструктурой организации
- Управление пользователями и их правами доступа
- Мультитенантность

Мониторинг и отчеты

- Настройка журналов на устройствах CPE
- Отслеживание информации о пакетах трафика с помощью протокола NetFlow
- Диагностика устройств CPE
- Мониторинг компонентов решения

Обновление

Обновите Kaspersky SD-WAN с предыдущей версии

Дополнительные возможности

- Управление межсетевым экраном
- Качество обслуживания (QoS)
- Зеркалирование трафика

Приложения

Получите информацию о Kaspersky SD-WAN из дополнительных руководств

О Kaspersky SD-WAN

Kaspersky SD-WAN используется для построения программно-определяемых глобальных сетей (англ. Software Defined WAN, далее сетей SD-WAN). В сетях SD-WAN автоматически определяются маршруты передачи трафика с наименьшей задержкой и наибольшей полосой пропускания. Для маршрутизации трафика применяется технология SDN (Software Defined Networking).

Технология SDN отделяет плоскость управления сетью (англ. control plane) от плоскости передачи данных (англ. data plane) и позволяет управлять сетевой инфраструктурой с помощью оркестратора (через веб-интерфейс или API). Благодаря отделению плоскости управления от плоскости передачи данных становится возможной *виртуализация сетевых функций* (англ. Network Function Virtualization, далее также NFV), в рамках которой сетевые функции, такие как межсетевые экраны, маршрутизаторы и балансировщики нагрузки, развертываются на стандартном оборудовании. Виртуализация сетевых функций в решении соответствует стандартам спецификации NFV MANO (NFV Management and Network Orchestration) Европейского института по стандартизации в области телекоммуникаций (англ. European Telecommunications Standards Institute, ETSI).

Построение сети SD-WAN не зависит от транспортных технологий. Вы можете использовать несколько соединений для передачи трафика с учетом требований приложений к пропускной способности и качеству обслуживания. Поддерживаются следующие типы нижележащей сети (англ. underlay network):

- транспортные сети MPLS;
- широкополосные каналы для подключения к интернету;
- арендуемые линии связи;
- беспроводные подключения, в том числе 3G, 4G и LTE;
- спутниковые каналы.

Решение предназначено для операторов связи (англ. service providers), а также организаций с крупной филиальной сетью, и заменяет стандартные маршрутизаторы в распределенных сетях устройствами Customer Premise Equipment (далее устройства CPE).

С помощью Kaspersky SD-WAN вы можете выполнять следующие задачи:

- интеллектуально управлять трафиком;
- автоматически настраивать устройства CPE;
- централизованно управлять компонентами решения с помощью веб-интерфейса;
- выполнять мониторинг сети;
- автоматически реагировать на изменение политик качества обслуживания, чтобы соответствовать требованиям приложений.

На рисунке ниже представлена схема сети SD-WAN, которая построена с помощью решения Kaspersky SD-WAN.



Схема сети SD-WAN

Комплект поставки

О приобретении решения вы можете узнать на сайте "Лаборатории Касперского" (https://www.kaspersky.ru) или у компаний-партнеров.

В комплект поставки входят следующие компоненты:

- Архив knaas-installer_<информация о версии> в формате TAR.GZ (далее также архив установки) для развертывания решения.
- Docker-контейнеры для развертывания компонентов Kaspersky SD-WAN:
  - knaas-ctl;
  - knaas-orc;
  - knaas-www;
  - knass-vnfm;
  - knaas-vnfm-proxy;
  - mockpnf.

  Следующие контейнеры вам нужно скачать из общего Docker-репозитория:
  - mariaDB;
  - mongo;
  - redis;
  - syslog-ng;
  - zabbix-proxy-mysql;
  - zabbix-server-mysql;
  - zabbix-web-nginx-mysql.
- Прошивки устройств CPE.
- Файл с текстом Лицензионного соглашения, в котором указано, на каких условиях вы соглашаетесь пользоваться решением.
- Файлы онлайн-справки Kaspersky SD-WAN для обеспечения возможности просмотра документации без подключения к интернету.

Состав комплекта поставки может отличаться в зависимости от региона, в котором распространяется решение.

Аппаратные и программные требования

Kaspersky SD-WAN имеет следующие аппаратные и программные требования:

Требования к аппаратным ресурсам зависят от количества управляемых устройств CPE (см. рекомендуемые схемы развертывания ниже). При необходимости рассчитать более точные аппаратные требования для определенной схемы развертывания мы рекомендуем обратиться в Службу технической поддержки "Лаборатории Касперского".

1. Рекомендуемые вычислительные ресурсы для компонентов решения версии 2.4 и выше

Ниже приведены поддерживаемые спецификации экземпляров оркестратора Kaspersky SD-WAN (ORC), контроллера Kaspersky SD-WAN (CTL), компонента мониторинга (MON) и утилиты Kaspersky Deployment Toolkit (KDT) при условии использования идентичных компонентов и версий ПО.

1.1. Оркестратор SD-WAN

Таблица 1. Определения типов экземпляров ORC

Тип экземпляра	Количество устройств CPE	Характеристики (приблизительно)				
		Процессор*	ОЗУ	Размер хранилища**	IOPS хранилища**	Сетевая карта
Small ORC	1000	16 ядер	32 ГБ	256 ГБ	3 000	2 x 1 Гбит/с
Medium ORC	5 000	24 ядра	64 ГБ	512 ГБ	5 000	2 x 1 Гбит/с
Large ORC	10 000	32 ядра	128 ГБ	1 ТБ	10 000	2 x 10 Гбит/с

* Процессор без Hyper-Threading. Рекомендации:

- Xeon Silver 4314 для экземпляров с типом Small ORC.
- Xeon Gold 5318Y или Gold 5418Y или выше для экземпляров с типом Medium ORC.
- Xeon Gold 6414U или Gold 6438Y+ или выше для экземпляров с типом Large ORC.

**SSD

1.2. Контроллер SD-WAN

Таблица 2.Определения типов экземпляров CTL

Тип экземпляра	Количество устройств CPE	Характеристики (приблизительно)				
		Процессор*	ОЗУ	Размер хранилища**	IOPS хранилища**	Сетевая карта
Small CTL	250	16 ядер	32 ГБ	64 ГБ	3 000	2 x 1 Гбит/с
Medium CTL	500	24 ядра	48 ГБ	128 ГБ	5 000	2 x 1 Гбит/с
Large CTL	1000	32 ядра	64 ГБ	256 ГБ	10 000	2 x 10 Гбит/с

* Процессор без Hyper-Threading. Рекомендации:

- Xeon Silver 4314 для экземпляров с типом Small CTL.
- Xeon Gold 5318Y или Gold 5418Y или выше для экземпляров с типом Medium CTL.
- Xeon Gold 6414U или Gold 6438Y+ или выше для экземпляров с типом Large CTL.

**SSD

1.3. Компонент мониторинга SD-WAN

Таблица 3. Определения типов экземпляров MON

Тип экземпляра	Количество устройств CPE	Характеристики (приблизительно)				
		Процессор*	ОЗУ	Размер хранилища**	IOPS хранилища**	Сетевая карта
Small MON	1 000	8 ядер	16 ГБ	1 ТБ	3 000	2 x 1 Гбит/с
Medium MON	5 000	24 ядра	64 ГБ	5 ТБ	5 000	2 x 1 Гбит/с
Large MON	10 000	32 ядра	96 ГБ	10 ТБ	10 000	2 x 10 Гбит/с

* Процессор без Hyper-Threading. Рекомендации:

- Xeon Silver 4309Y для экземпляров с типом Small MON.
- Xeon Gold 5318Y или Gold 5418Y или выше для экземпляров с типом Medium MON.
- Xeon Gold 6414U или Gold 6438Y+ или выше для экземпляров с типом Large MON.

**SSD, RAID 10

1.4. SD-WAN All-in-One

Экземпляр типа SD-WAN All-in-One (AIO, "все-в-одном") включает в себя следующие компоненты администрирования: оркестратор Kaspersky SD-WAN (ORC), контроллер Kaspersky SD-WAN (CTL) и компонент мониторинга Kaspersky SD-WAN (MON). Поддерживаются следующие спецификации экземпляров:

Таблица 4. Определения типов экземпляров AIO

Тип экземпляра	Количество устройств CPE	Характеристики (приблизительно)				
		Процессор*	ОЗУ	Размер хранилища**	IOPS хранилища**	Сетевая карта
Small AIO	50	16 ядер	32 ГБ	256 ГБ	3 000	1 Гбит/с
Medium AIO	100	24 ядра	48 ГБ	512 ГБ	5 000	2 x 1 Гбит/с
Large AIO	250	32 ядра	64 ГБ	1024 ГБ	10 000	2 x 10 Гбит/с

1.5. Хост для развертывания SD-WAN

Для развертывания и обновления управляющих компонентов решения по схемам "Высокая доступность" (High Availability) и "Распределенное развертывание" (Distributed Deployment) требуется выделенный хост с Kaspersky Deployment Toolkit (KDT).

Таблица 5. Определения типов экземпляров KDT

Схема развертывания	Характеристики (приблизительно)				
	Процессор*	ОЗУ	Размер хранилища**	IOPS хранилища**	Сетевая карта
Высокая доступность и распределенное развертывание	8 ядер	16 ГБ	512 ГБ	5 000	1 Гбит/с

* Процессор без Hyper-Threading. Рекомендации:

- Xeon Silver 4309Y для экземпляров с типом KDT.

**SSD

2. Схемы развертывания системы администрирования

2.1. Автономное развертывание

Схема автономного развертывания системы администрирования Kaspersky SD-WAN предназначена только для демонстрационных целей и не рекомендуется для использования в продуктовой среде.

2.2. Развертывание с высокой доступностью (High Availability Deployment)

Для развертывания системы администрирования Kaspersky SD-WAN по схеме с высокой доступностью (High Availability, HA) требуется три экземпляра AIO (HA3). Аппаратные характеристики экземпляров приведены в таблице 4. В таблице ниже приведены рекомендации по масштабированию при развертывании по схеме HA3.

Таблица 6. Характеристики экземпляров для развертывания по схеме HA3

Количество устройств CPE	Экземпляр HA3
50	3 x Small AIO
100	3 x Medium AIO
250	3 x Large AIO

2.3. Распределенное развертывание (Distributed Deployment)

Для развертывания системы администрирования Kaspersky SD-WAN по схеме распределенного развертывания требуется три выделенных экземпляра ORC, три выделенных экземпляра CTL, три выделенных экземпляра MON и один хост KDT.

Таблица 7. Характеристики экземпляров для развертывания

Количество устройств CPE	ORC	CTL	MON	KDT
250	3 x Small ORC	3 x Small CTL	3 x Small MON	1 x KDT
500	3 x Small ORC	3 x Medium CTL	3 x Small MON	1 x KDT
1 000	3 x Small ORC	3 x Large CTL	3 x Small MON	1 x KDT
2 500	3 x Small ORC	15 x Medium CTL	3 x Small MON	1 x KDT
5 000	3 x Medium ORC	30 x Medium CTL	3 x Medium MON	1 x KDT
7 500	3 x Medium ORC	45 x Medium CTL	3 x Medium MON	1 x KDT
10 000	3 x Large ORC	60 x Medium CTL	3 x Large MON	1 x KDT
20 000	6 x Large ORC	120 x Medium CTL	6 x Large MON	1 x KDT
25 000	9 x Large ORC	150 x Medium CTL	9 x Large MON	1 x KDT

3. Требования к сторонним решениям

Для развертывания Kaspersky SD-WAN необходимы следующие сторонние решения:

- Платформа Docker версии 1.5 или выше для развертывания Docker-контейнеров компонентов решения. Более подробную информацию вы можете получить из официальной документации платформы Docker.
- Система мониторинга Zabbix версии 5.0.26 и 6.0.0. Более подробную информацию вы можете получить из официальной документации решения Zabbix.
- Сервис OpenStreetMap для просмотра топологии транспортных сервисов поверх карты. Если инфраструктура вашей организации не предусматривает выхода в интернет, вы можете использовать офлайн-карты. Офлайн-карты занимают дополнительное дисковое пространство:
  - офлайн-карта (central-fed-district-latest.osm.pbf) занимает около 100 ГБ;
  - данные для геокодинга занимают около 10 ГБ.

  Более подробную информацию вы можете получить из официальной документации сервиса OpenStreetMap.

Требования к операционным системам

Поддерживаются следующие 64-разрядные операционные системы:

- Ubuntu версии 22.04 LTS.
- Astra Linux версии 1.7 (уровень защищенности: "Орел").
- РЕД ОС 7.3 "МУРОМ".

Требования к каналам связи между узлами компонентов решения

При развертывании Kaspersky SD-WAN вы можете развернуть несколько узлов компонентов решения. Существуют следующие требования к каналам связи между узлами компонентов решения:

- Требования к каналам связи между узлами контроллера:
  - пропускная способность – 1 Гбит/сек.;
  - RTT (Round Trip Time) – не более 200 мс;
  - потеря пакетов – 0%.
- Требования к каналам связи между узлами базы данных MongoDB:
  - пропускная способность – 1 Гбит/сек.;
  - RTT – не более 50 мс;
  - потеря пакетов – 0%.
- Требования к каналам связи между узлами базы данных Redis:
  - пропускная способность – 1 Мбит/сек.;
  - RTT – не более 50 мс;
  - потеря пакетов – 0%.

Требования к браузерам

Поддерживаются следующие браузеры для работы с веб-интерфейсом оркестратора:

- Google Chrome версии 100 и выше.
- Firefox версии 100 и выше.
- Microsoft Edge версии 100 и выше.
- Opera версии 90 и выше.
- Safari версии 15 и выше.

Требования к устройствам CPE

Поддерживаются следующие модели устройств CPE:

- 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.

Устройства CPE модели KESR основаны на архитектурах процессоров x86 (Intel 80x86) и MIPS (Microprocessor without Interlocked Pipeline Stages).

На устройствах CPE модели KESR M3–M5 установлены сетевые карты компании Intel, совместимые с SFP-трансиверами компании Intel. Более подробную информацию о поддерживаемых SFP-трансиверах можно получить с помощью инструмента Intel Product Compatibility Tool (на территории Российской Федерации ссылка доступна только через VPN). При работе с инструментом Intel Product Compatibility Tool вам нужно выбрать одну из следующих категорий продукта:

- **500 Series** – для просмотра SFP-трансиверов, совместимых с устройствами CPE модели KESR M3.
- **700 Series** – для просмотра SFP-трансиверов, совместимых с устройствами CPE моделей KESR M4–M5.

Специалисты "Лаборатории Касперского" протестировали работоспособность устройств CPE при предоставлении услуги L3 VPN (см. таблицу ниже). На тестируемых устройствах не использовалась технология DPI (Deep Packet Inspection) и было выключено шифрование трафика.

Модель	Размер пакетов (байт)	Пропускная способность, МБ/сек.
KESR-M1	IMIX (417)	30
	Large (1300)	115
KESR-M2	IMIX (417)	165
	Large (1300)	241
KESR-M3	IMIX (417)	805
	Large (1300)	1150
KESR-M4	IMIX (417)	1430
	Large (1300)	2870

Более подробная информация о характеристиках устройств CPE содержится на официальной странице решения.

Вы можете развертывать устройства uCPE на серверах с архитектурами процессоров x86 (Intel 80x86) и ARM64.

Требования к устройствам vCPE

В комплекте поставки содержатся следующие прошивки для развертывания устройств vCPE:

- vKESR-M1.
- vKESR-M2.

- vKESR-M3.
- vKESR-M4.

Для устройств vCPE поддерживаются следующие среды виртуализации:

- Среда виртуализации VMware версии 7.0 и выше.
- Среда виртуализации KVM с версией ядра 5.15 и выше.

> Поддерживается только оригинальная среда виртуализации KVM без дополнительных средств оркестрации.

Требования к виртуальным ресурсам для развертывания устройств vCPE описаны в таблице ниже.

Прошивка	Процессор	ОЗУ, ГБ	Диск, ГБ
vKESR-M1	2	0.5	1
vKESR-M2	4	8	1
vKESR-M3	12	16	1
vKESR-M4	24	32	1

При обновлении Kaspersky SD-WAN с версии 2.2 до 2.3 вам нужно привести ранее развернутые устройства vCPE к текущим требованиям, после чего вы сможете обновить устройства vCPE, используя прошивки vKESR-M1–5.

Обеспечение безопасности

Безопасность в Kaspersky SD-WAN обеспечивается в плоскостях передачи данных, управления сетью и оркестрации. Степень безопасности всего решения определяется степенью безопасности каждой из этих плоскостей, а также защищенностью взаимодействия между ними. В каждой плоскости происходят следующие процессы:

- аутентификация и авторизация пользователей;
- использование безопасных протоколов управления;
- шифрование управляющего трафика;
- безопасное подключение устройств CPE.

Безопасные протоколы управления

Мы рекомендуем использовать протокол HTTPS при взаимодействии с сетью SD-WAN через веб-интерфейс оркестратора или API. Вы можете загрузить в веб-интерфейс собственные сертификаты или использовать автоматически сгенерированные самоподписанные сертификаты. Решение использует несколько протоколов для передачи управляющего трафика компонентам (см. таблицу ниже).

Взаимодействующие компоненты	Проткол	Дополнительное обеспечение безопасности
Оркестратор и контроллер	gRPC	Для аутентификации и шифрования трафика между клиентом и сервером используется протокол TLS.
Оркестратор и устройство CPE	HTTPS	Для аутентификации и шифрования трафика между оркестратором и устройством CPE используется проверка сертификата и токен.
Контроллер и устройство CPE	OpenFlow 1.3.4	Для аутентификации и шифрования трафика между контроллером и устройством CPE используется протокол TLS.

Безопасное подключение устройств CPE

Решение использует следующие механизмы безопасного подключения устройств CPE:

- Обнаружение устройств CPE с помощью идентификаторов DPID (datapath identifier).
- Отложенная регистрация. Вы можете выбрать, в каком состоянии находится устройство CPE после успешной регистрации – **Включено** или **Выключено**. Выключенное устройство CPE необходимо включить, убедившись, что оно установлено на площадке.
- Двухфакторная аутентификация.

Использование виртуальных сетевых функций

Вы можете обеспечить дополнительный уровень безопасности с помощью виртуальных сетевых функций, развертываемых в центре обработки данных и/или на uCPE. Например, трафик может быть направлен от устройства CPE к виртуальной сетевой функции, которая работает как межсетевой экран или прокси-сервер. Виртуальные сетевые функции могут выполнять следующие функции защиты сети SD-WAN:

- межсетевой экран нового поколения (англ. Next-Generation Firewall, NGFW);
- защита от атак DDoS (Distributed Denial of Service);
- системы обнаружения и предотвращения вторжений IDS (Intrusion Detection System) и IPS (Intrusion Prevention System);
- антивирус;
- антиспам;
- система фильтрации веб-адресов и контента;
- система защиты от утечек конфиденциальных данных DLP (Data Loss Prevention);
- веб-прокси Secure Web Proxy.
-

Что нового

В Kaspersky SD-WAN появились следующие возможности и доработки:

- Перенаправление DNS-запросов в зависимости от условий.
- Сбор отладочной информации для протоколов BGP и OSPF через оркестратор.
- Отложенное применение конфигурации CPE.
- Балансировка между оркестраторами.
- Замена устройств CPE с сохранением настроек.
- Диагностика LTE через оркестратор.
- Централизованная настройка поведения при подключении к устройствам CPE через консольный порт.
- Динамическое распределение трафика транспортного сервиса по нескольким путям на основе мониторинга потерь трафика по каждому пути.
- Массовый импорт DPID устройств CPE из файла.
- Получение порта подключения CPE к оркестратору по протоколу DNS.
- Максимальное количество поддерживаемых CPE для оркестратора увеличено до 2000+.
- Возможность указать индекс интерфейса при отправке NetFlow.
- Система индикации о сбоях по питанию CPE (только для специальных исполнений CPE).

Известные ограничения

Kaspersky SD-WAN имеет следующие ограничения:

- Ограничения при интеграции решения с Kaspersky KSC/OSMP:
  - доступно только для новых инсталляций;
  - не поддерживается ssh-консоль;
  - не поддерживается vnc-консоль.
- Правила межсетевого экрана не учитывают созданные пользователями виртуальные таблицы маршрутизации (нельзя задать правила с сопоставлением по виртуальной таблице маршрутизации, вместо этого необходимо использовать другие признаки, такие как интерфейсы, IP-адреса и т.п.).
- При изменении статических маршрутов возможна перезагрузка демона FRR.
- Переключение режимов модема между LTE и 3G (UMTS, CDMA, TD-SCDMA) может вызвать разрыв в графиках диагностики, так как для LTE доступны параметры RSSI, RSRQ, RSRP, SNR, а для 3G – только RSSI и ECIO.

Архитектура решения

Kaspersky SD-WAN содержит следующие основные компоненты:

- Оркестратор

  Контролирует инфраструктуру решения, выполняет функции оркестратора NFV (NFVO), а также управляет сетевыми сервисами и распределенными менеджерами VNF (VNFM). Вы можете управлять оркестратором с помощью веб-интерфейса и REST API при использовании внешних северных (англ. northbound) систем.

- Контроллер

  Централизованно управляет наложенной сетью:

  - строит сетевую топологию;
  - создает транспортные сервисы;
  - управляет устройствами CPE по протоколу OpenFlow;
  - распределяет трафик между соединениями;
  - обеспечивает мониторинг соединений и автоматически переключает трафик на резервное соединение, если основное соединение выходит из строя.

  Для развертывания контроллера вам нужно развернуть физическую сетевую функцию контроллера, которая содержится в архиве установки. Контроллер управляется оркестратором.

- Устройства CPE

  Устанавливаются на удаленных площадках, передают трафик и образуют SDN-фабрику в виде наложенной сети. Вы можете назначить устройству CPE роль шлюза SD-WAN или стандартного устройства CPE. Шлюзы SD-WAN строят соединения со всеми стандартными устройствами CPE и другими шлюзами SD-WAN. Стандартные устройства CPE строят соединения только со шлюзами SD-WAN. По умолчанию всем устройствам CPE назначена роль стандартных устройств CPE.

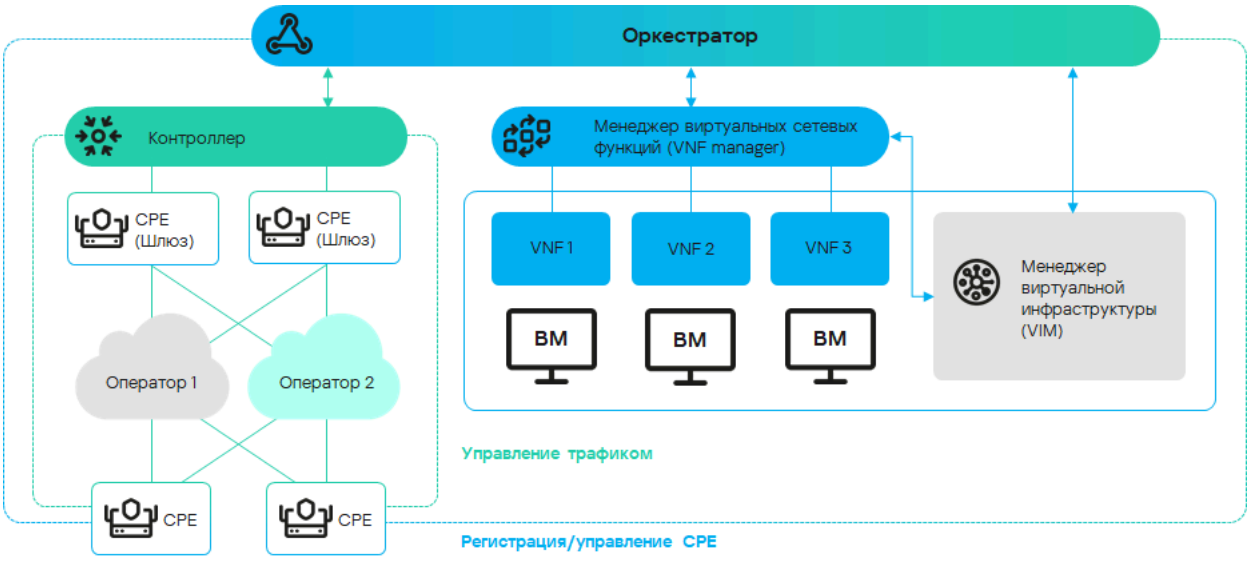
  Если вы хотите, чтобы между двумя стандартными устройствами CPE было построено соединение, вам нужно назначить им одинаковый топологический тег. Вы можете сделать стандартное устройство CPE транзитным, чтобы другие устройства CPE могли строить через него соединения.

- VNFM (Virtual Network Function Manager)

  Управляет жизненным циклом виртуальных сетевых функций с помощью SSH, плейбуков Ansible, скриптов и атрибутов Cloud-init.

При использовании виртуальных сетевых функций в архитектуру решения входит менеджер виртуальной инфраструктуры (Virtual Infrastructure Manager, далее также VIM), который управляет вычислительными и сетевыми ресурсами, а также ресурсами хранения в рамках инфраструктуры NFV. VIM связывает виртуальные сетевые функции с помощью виртуальных соединений, подсетей и портов. В качестве VIM используется облачная платформа OpenStack.

Kaspersky SD-WAN имеет распределенную микросервисную архитектуру на основе Docker-контейнеров (см. рисунок ниже). Контроллер может состоять из одного, трех или пяти узлов. Узлы контроллера можно развернуть на отдельных виртуальных машинах или физических серверах, чтобы обеспечить отказоустойчивость. Вы можете указать виртуальные машины или физические сервера для развертывания узлов контроллера при развертывании решения в блоке `ctl` конфигурационного файла.



Архитектура Kaspersky SD-WAN

Развертывание Kaspersky SD-WAN

Вы можете развернуть Kaspersky SD-WAN с помощью архива установки knaas-installer_<информация о версии>, который содержится в комплекте поставки. Перед выполнением этого сценария вам нужно составить схему развертывания решения. При возникновении проблем с составлением схемы развертывания мы рекомендуем обратиться в техническую поддержку "Лаборатории Касперского".

Сценарий развертывания решения состоит из следующих этапов:

1. **Подготовка устройства администратора**

   Подготовьте устройство администратора для развертывания решения. Устройство администратора может быть локальной или удаленной виртуальной машиной, а также персональным компьютером. При развертывании демонстрационного стенда Kaspersky SD-WAN в соответствии со схемой развертывания все-в-одном в качестве устройства администратора необходимо использовать виртуальную машину.

2. **Обеспечение сетевой связности между устройством администратора компонентами решения**

   Обеспечьте сетевую связность между устройством администратора и виртуальными машинами или физическими серверами, на которых вы хотите развернуть компоненты Kaspersky SD-WAN. Если вы планируете развернуть несколько узлов компонентов решения, вам нужно убедиться, что каналы связи между виртуальными машинами или физическими серверами соответствуют аппаратным и программным требованиям.

   > Виртуальные машины или физические серверы необходимо развернуть в доверенном сетевом сегменте, чтобы избежать компрометации передаваемого трафика.

3. **Ручная генерация паролей**

   При необходимости вручную сгенерируйте пароли для обеспечения безопасности компонентов Kaspersky SD-WAN и их SSL-сертификатов.

4. **Настройка конфигурационного файла**

   Настройте конфигурационный файл в соответствии с выбранной схемой развертывания. Вы можете использовать примеры конфигурационных файлов для типовых схем развертывания, которые содержатся в директориях /inventory/external/pnf и /inventory/external/vnf архива установки.

5. **Изменение графических элементов веб-интерфейса оркестратора**

   При необходимости измените графические элементы веб-интерфейса оркестратора. Например, вы можете изменить изображение, которое отображается на фоне, когда возникает ошибка при входе в веб-интерфейс оркестратора.

6. **Развертывание Kaspersky SD-WAN**

   Выполните следующие действия на устройстве администратора:

   1. Примите Лицензионное соглашение, выполнив команду:

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

   2. Перейдите в распакованный архив установки.

   3. Если вы хотите развернуть Kaspersky SD-WAN в режиме attended, выполните одно из следующих действий:

- Если вы сгенерировали вручную пароли, выполните команду:

  ```
  ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
  ```

  При выполнении команды введите пароль учетной записи root и сгенерированный мастер-пароль.

- Если вы не сгенерировали вручную пароли, выполните команду:

  ```
  ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e "@inventory/external/images.yml" -K knaas/knaas-install.yml
  ```

4. Если вы хотите развернуть Kaspersky SD-WAN в режиме unattended, выполните одно из следующих действий:

   Мы рекомендуем использовать этот режим только в доверенной среде, так как в противном случае злоумышленники могут перехватить ваши пароли.

   - Если вы сгенерировали вручную пароли, выполните команду:

     ```
     ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
     ```

   - Если вы не сгенерировали вручную пароли, выполните команду:

     ```
     ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" knaas/knaas-install.yml
     ```

   Компоненты Kaspersky SD-WAN будут развернуты на виртуальных машинах или физических серверах, которые вы указали в конфигурационном файле. Сообщение об успешном развертывании отобразится в консоли устройства администратора.

Если при развертывании компонентов решения возникает проблема сетевой связности с одной из виртуальных машин или с одним из физических серверов, в консоли устройства администратора отображается ошибка и решение не развертывается. В этом случае вам нужно восстановить сетевую связность, очистить виртуальные машины или физические серверы, после чего заново выполнить команду развертывания.

Резервирование компонентов решения

О схемах резервирования компонентов решения

Kaspersky SD-WAN поддерживает две схемы развертывания компонентов решения:

- *N+1* – вы развертываете два узла компонента решения. Если один узел выходит из строя, работу компонента решения обеспечивает второй узел.
- *2N+1* – вы развертываете несколько узлов компонентов решения. Один узел является основным, а другие – второстепенными. Если основной узел выходит из строя, его место занимает случайно выбранный второстепенный узел. Такая схема резервирования позволяет компонентам решения сохранять работоспособность, даже когда происходит несколько аварий подряд.

В таблице ниже представлены компоненты решения и доступные для них схемы развертывания.

Компонент решения	Схема резервирования
База данных системы мониторинга Zabbix	2N+1
Сервер Zabbix	N+1
Frontend-часть системы мониторинга Zabbix	N+1
Сервер Zabbix-прокси	N+1
База данных MongoDB	2N+1
База данных Redis: • сервер Redis replica; • система Redis Sentinel.	2N+1
Контроллер	2N+1
Frontend-часть решения	N+1
Оркестратор	N+1
Менеджер виртуальных сетевых функций	N+1
Прокси-менеджер виртуальных сетевых функций	N+1

Вы можете указать, сколько узлов развертывается для компонентов решения в конфигурационном файле.

Когда вы настраиваете параметры развертывания узлов базы данных MongoDB или контроллера в соответствии со схемой развертывания 2N+1, последний указанный вами узел становится узлом-арбитром. *Узел-арбитр* связан с другими узлами и используется для выбора основного узла. Узел, который потерял связь с узлом-арбитром, переходит в режим ожидания. Один из узлов, которые сохранили связь с узлом-арбитром, остается или становится основным узлом. Узел-арбитр не может стать основным узлом и не хранит данные.

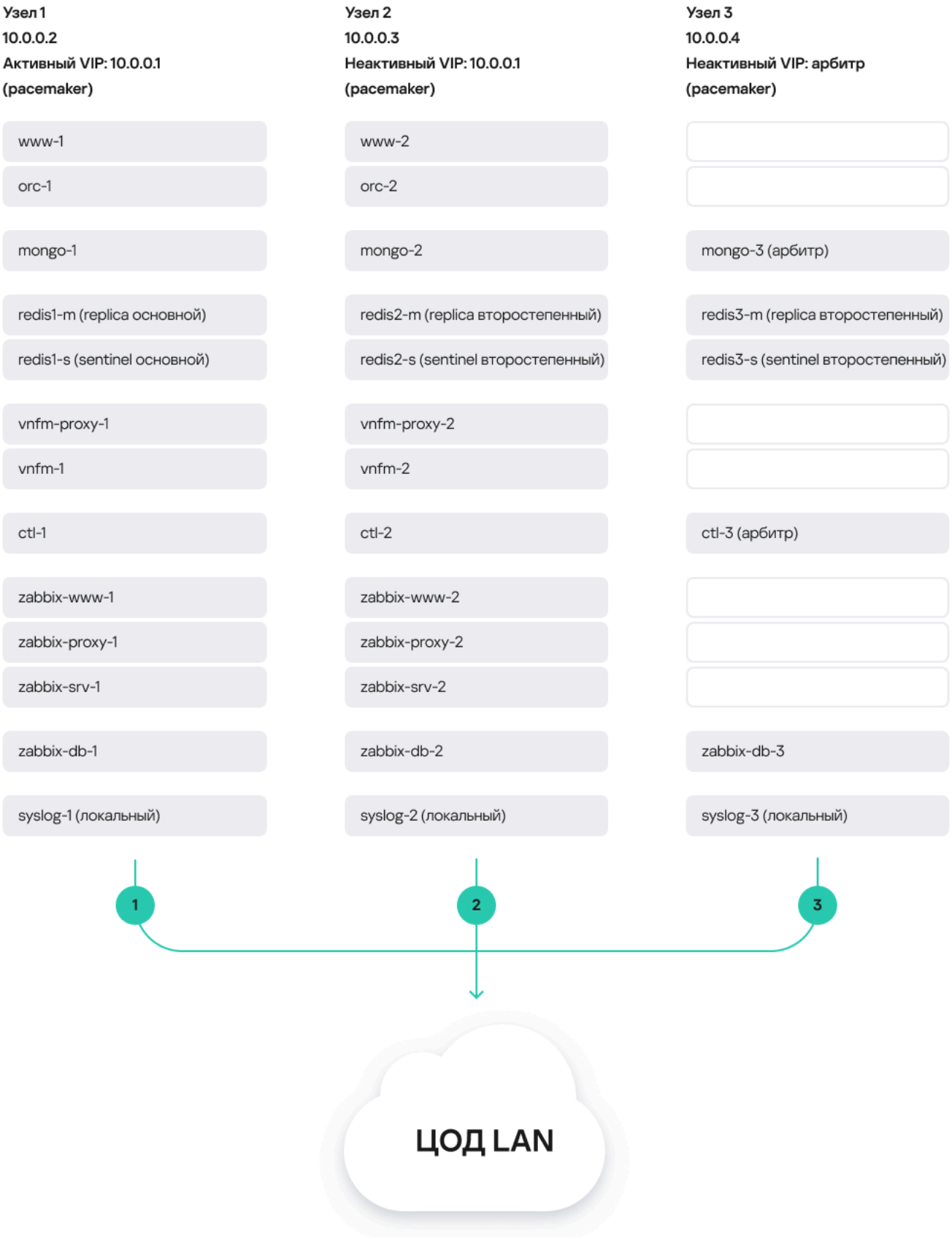
Сценарии выхода из строя узлов компонентов решения

На рисунке ниже изображена схема Kaspersky SD-WAN, развернутого на трех виртуальных машинах в центре обработки данных. В схеме используются следующие условные обозначения:

- www – frontend-часть решения;
- orc – оркестратор;
- mongo – база данных MongoDB;
- redis-m – сервер Redis replica;
- redis-s – система Redis Sentinel;
- vnfm-proxy – прокси-менеджер виртуальных сетевых функций;
- vnfm – менеджер виртуальных сетевых функций;
- ctl – контроллер и его база данных;
- zabbix-www – frontend-часть системы мониторинга Zabbix;
- zabbix-proxy – сервер Zabbix-прокси;

- zabbix-srv – сервер Zabbix;
- zabbix-db – база данных системы мониторинга Zabbix;
- syslog – syslog-сервер.

Пользователи и устройства CPE получают доступ к веб-интерфейсу оркестратора и веб-интерфейсу системы мониторинга Zabbix с помощью виртуального IP-адреса. Виртуальный IP-адрес назначен виртуальной машине 1.



Решение, развернутое на трех виртуальных машинах

В рамках представленной схемы развертывания возможны следующие сценарии аварийных ситуаций:

- **Выход из строя виртуальной машины 1 или ее соединения**.

  При выходе из строя виртуальной машины 1 или ее соединения решение сохраняет работоспособность. Происходят следующие изменения состояния узлов компонентов решения:

  - Виртуальный IP-адрес назначается виртуальной машине 2.
  - Узел frontend-части решения www-1 недоступен, www-2 доступен. Веб-интерфейс оркестратора отображается в браузере.
  - Узел оркестратора orc-1 недоступен, orc-2 доступен. Backend-часть решения работает, пользователи могут войти в веб-интерфейс оркестратора и использовать его.
  - Узел базы данных MongoDB mongo-1 недоступен, mongo-2 и mongo-3 доступны, mongo-2 становится основным узлом, так как mongo-3 является узлом-арбитром и не может стать основным узлом. Оркестратор продолжает использовать базу данных MongoDB.
  - Состояние базы данных Redis:
    - Узел сервера Redis replica redis1-m недоступен, redis2-m и redis3-m доступны.
    - Узел системы Redis Sentinel redis1-s недоступен, redis2-s и redis3-s доступны, redis2-s становится основным узлом и случайным образом назначает узел сервера Redis replica redis2-m или redis3-m основным узлом.

    Оркестратор продолжает использовать базу данных Redis.
  - Состояния менеджера виртуальных сетевых функций:
    - Узел прокси-менеджера виртуальных сетевых функций vnfm-proxy-1 недоступен, vnfm-proxy-2 доступен.
    - Узел менеджера виртуальных сетевых функций vnfm-1 недоступен, vnfm-2 доступен.

    SSH-консоли компонентов решения работают.
  - Узел контроллера ctl-1 недоступен, ctl-2 и ctl-3 доступны, ctl-2 становится основным узлом, так как ctl-3 является узлом-арбитром и не может стать основным узлом. Сохраняется сетевая связность между устройствами CPE.
  - Состояние системы мониторинга Zabbix:
    - Узел frontend-части решения zabbix-www-1 недоступен, zabbix-www-2 доступен.
    - Узел сервера Zabbix-прокси zabbix-proxy-1 недоступен, zabbix-proxy-2 доступен.
    - Узел сервера Zabbix zabbix-srv-1 недоступен, zabbix-srv-2 доступен.
    - Узел базы данных системы мониторинга Zabbix zabbix-db-1 недоступен, zabbix-db-2 доступен.

    Система мониторинга Zabbix работает.

- **Выход из строя виртуальной машины 2 или 3, или ее соединения**.

При выходе из строя виртуальной машины 2 или 3, или ее соединения узлы компонентов решения, развернутые на виртуальной машине 1, остаются основными и решение сохраняет работоспособность.

- **Одновременный выход из строя виртуальных машин 1 и 3 или 2 и 3, или их соединений**

  При одновременном выходе из строя виртуальных машин 1 и 3 или 2 и 3, или их соединений решение не сохраняет работоспособность. Происходят следующие изменения состояния узлов компонентов решения:

  - Веб-интерфейс оркестратора не отображается в браузере. Пользователи не могут войти в веб-интерфейс оркестратора и использовать его.
  - Система мониторинга Zabbix прекращает работу.
  - Сохраняется сетевая связность между устройствами CPE и подключенными к ним сетевыми устройствами, трафик продолжает передаваться.
  - Сохраняется сетевая связность в рамках P2P-сервисов и TAP-сервисов.
  - Сохраняется сетевая связность в рамках P2M-сервисов и M2M-сервисов для установленных сессий. Для новых сессий сетевая связность сохраняется, если при создании P2P-сервиса или M2M-сервиса в раскрывающемся списке **Режим изучения MAC** вы выбрали значение **Learn and flood**.
  - Устройства CPE используют механизм компенсации реордеринга (англ. reordering) для снижения количества дублированных пакетов на сетевых устройствах, подключенных к устройствам CPE.
  - Нагрузка на устройства CPE и сеть SD-WAN возрастает соразмерно количеству устройств CPE и соединений.

  Если соединения восстанавливаются, решение также восстанавливается и продолжает работать в нормальном режиме.

  При одновременном выходе из строя виртуальных машин 1 и 3 или 2 и 3 происходит потеря конфигурации компонентов решения. Для восстановления конфигурации компонентов решения вы можете обратиться в Kaspersky Professional Services.

- **Одновременный выход из строя виртуальных машин 1 и 2**

  При одновременном выходе из строя виртуальных машин 1 и 2 происходит потеря конфигурации компонентов решения без возможности восстановления, так как на виртуальной машине 3 развернуты узлы-арбитры, которые не хранят данные. Для предотвращения такой ситуации мы рекомендуем развертывать базы данных и контроллеры на отдельных виртуальных машинах или физических серверах и делать регулярные резервные копии.

Настройка балансировки нагрузки между экземплярами оркестратора

Для увеличения производительности в продуктовых средах с большим количеством устройств CPE при развертывании решения предусмотрена возможность создания нескольких экземпляров контейнера оркестратора для распределения нагрузки между ними. Каждый экземпляр контейнера оркестратора может обслуживать до 5000 устройств CPE.

Экземпляры контейнера объединяются в *группы балансировки*. Группа балансировки включает в себя один контейнер `www` и от одного до пяти контейнеров оркестратора. Количество групп балансировки зависит от схемы развертывания: 1 в случае схемы "все-в-одном", 2 в случае схемы с высокой доступностью. Название контейнеров соответствует шаблону `orc-nm`, где `n` означает номер группы балансировки, `m` означает порядковый номер экземпляра контейнера в группе, если используется больше одного экземпляра. Примеры: `orc-12` (контейнер первой группы балансировки, второй экземпляр); `orc-2` (единственный контейнер второй группы балансировки).

При развертывании Kaspersky SD-WAN возможен один из двух вариантов развертывания групп балансировки:

- Контейнер `www` и контейнеры оркестратора группы балансировки разворачиваются на одном и том же узле.

  Чтобы выбрать этот вариант развертывания группы балансировки, при настройке конфигурационного файла необходимо указать в переменной `number_of_containers` количество контейнеров, которые необходимо развернуть для группы балансировки на соответствующем узле (от 1 до 5).

- Контейнер `www` и каждый из контейнеров оркестратора группы балансировки разворачиваются на отдельном узле.

  Этот вариант можно использовать для горизонтального масштабирования и более удобной утилизации ресурсов. Чтобы выбрать этот вариант развертывания группы балансировки, при настройке конфигурационного файла необходимо в переменной `ansible_host` секций `orc_1` и `orc_2` перечислить нужные узлы из секции `nodes`, на которых необходимо развернуть экземпляры контейнеров оркестратора. На каждом указанном узле можно развернуть только один экземпляр контейнера оркестратора.

  Если в переменной `ansible_host` указано больше одного узла, то значение переменной `number_of_containers` игнорируется.

Об архиве установки

Архив установки knaas-installer_<информация о версии> имеет формат TAR и используется для развертывания решения. Вы можете скачать архив установки из корневой директории комплекта поставки. Архив установки имеет следующую структуру:

Мы не рекомендуем изменять системные файлы, так как это может привести к ошибкам при развертывании решения.

- ansible.cfg – системный файл с параметрами Ansible.
- CHANGELOG.md – журнал изменений файлов в формате YAML.
- /docs – документация по использованию архива установки.
- /images – образы компонентов решения.
- /inventory:
  - /external:
    - /pnf – примеры конфигурационных файлов для типовых схем развертывания решения с контроллером в виде физической сетевой функции.
    - /vnf – примеры конфигурационных файлов для типовых схем развертывания решения с контроллером в виде виртуальной сетевой функции.
- /generic – общие системные файлы.
- /knaas – системные файлы с плейбуками для развертывания решения.
- /oem – графические элементы по умолчанию веб-интерфейса оркестратора.
- /pnfs – физические сетевые функции для развертывания одного, трех или пяти узлов контроллера.
- README.md – инструкция по развертыванию решения с помощью архива установки.
- requirements.txt – системный файл с требованиями для Python.

О режимах выполнения действий attended, unattended и partially attended

Когда вы выполняете действия на устройстве администратора при развертывании Kaspersky SD-WAN, вам может потребоваться ввести пароль учетной записи root, а также мастер-пароль. Способ введения паролей определяется режимом, в котором вы выполняете действие. Поддерживаются следующие режимы выполнения действий:

- attended – действие выполняется с привлечением сотрудника. При выполнении действия вам нужно вручную ввести пароль учетной записи root и мастер-пароль. Это самый безопасный режим, при использовании которого ни один из паролей не сохраняется на устройстве администратора.
- unattended – действие выполняется без привлечения сотрудника. При выполнении действия пароль учетной записи root и мастер-пароль вводятся автоматически. В этом режиме вы можете проводить автоматизированные тесты.

  Мы рекомендуем использовать этот режим только в доверенной среде, так как в противном случае злоумышленники могут перехватить ваши пароли.

- partially attended – действие выполняется с частичным привлечением сотрудника. При выполнении действия вам нужно ввести пароль пользователя root, а мастер-пароль вводится автоматически.

Подготовка устройства администратора

Устройство администратора может быть локальной или удаленной виртуальной машиной, а также персональным компьютером. При развертывании демонстрационного стенда Kaspersky SD-WAN в соответствии со схемой развертывания все-в-одном в качестве устройства администратора необходимо использовать виртуальную машину.

Если при подготовке устройства администратора у вас возникают проблемы, мы рекомендуем обратиться в техническую поддержку "Лаборатории Касперского".

Чтобы подготовить устройство администратора:

1. Убедитесь, что устройство администратора соответствует аппаратным и программным требованиям.
2. Убедитесь, что на устройстве администратора и виртуальных машинах или физических серверах, на которых вы хотите развернуть компоненты Kaspersky SD-WAN, используется одинаковая учетная запись root. После развертывания решения вы можете использовать другую учетную запись root на виртуальных машинах или физических серверах.
3. Скачайте архив установки knaas-installer_<информация о версии> из корневой директории комплекта поставки и распакуйте архив установки на устройстве администратора.

4. Перейдите в распакованный архив установки и подготовьте устройство администратора:

   a. Убедитесь, что установлен инструмент управления пакетами pip, выполнив команду:

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

   b. При отсутствии инструмента управления пакетами pip выполните одно из следующих действий:

      - Если на устройстве администратора установлена операционная система Ubuntu, выполните команду:

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

      - Если на устройстве администратора установлена операционная система РЕД ОС 8, выполните команду:

        ```
        yum install python3-pip
        ```

   c. Установите инструмент Ansible и его зависимости, выполнив команду:

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

   d. Обновите переменную PATH, выполнив команды:

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

   e. Убедитесь, что инструмент Ansible готов к использованию, выполнив команду:

      ```
      ansible --version
      ```

   f. Установите на устройстве администратора пакеты операционной системы для развертывания Kaspersky SD-WAN, выполнив команду:

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

      При выполнении команды введите пароль учетной записи root.

Вам нужно выполнить этот шаг только при изначальном развертывании решения.

5. Убедитесь, что устройство администратора готово к использованию:

   a. Перезагрузите устройство администратора.

   b. Перейдите в распакованный архив установки и запустите автоматическую проверку устройства администратора, выполнив команду:

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

6. Если вы планируете развернуть Kaspersky SD-WAN на нескольких виртуальных машинах или физических серверах, выполните следующие действия:

   a. Убедитесь, что на устройстве администратора сгенерированы SSH-ключи. Если SSH-ключи не сгенерированы, сгенерируйте их.

   b. Поместите SSH-ключи на виртуальные машины или физические серверы, выполнив команду:

   ```
   ssh-copy-id user@< IP-адрес виртуальной машины или физического сервера >
   ```

   Если вы развертываете демонстрационный стенд Kaspersky SD-WAN в соответствии со схемой развертывания все-в-одном, пропустите этот шаг.

Устройство администратора будет подготовлено к развертыванию Kaspersky SD-WAN.

Работа с паролями

Безопасность развернутых компонентов Kaspersky SD-WAN обеспечивают пароли. Вы можете сгенерировать пароли вручную. Если вы не генерируете пароли вручную, они генерируются автоматически при развертывании решения.

Пароли содержатся в следующих файлах:

- keystore.yml – пароли компонентов Kaspersky SD-WAN и их SSL-сертификатов.
- vault_password.txt – мастер-пароль.

Мы рекомендуем хранить файлы с паролями в защищенной директории, так как с их помощью злоумышленники могут получить доступ к развернутому решению.

После развертывания сгенерированные пароли автоматически помещаются в Docker-контейнеры компонентов Kaspersky SD-WAN. При взаимодействии друг с другом компоненты решения обмениваются паролями.

Ручная генерация паролей

Чтобы вручную сгенерировать пароли:

1. Создайте директорию /passwords на устройстве администратора. Вам нужно указать путь к созданной директории в блоке `external` конфигурационного файла с помощью параметра `vault_password_dirname`.

2. Создайте файл keystore.yml и укажите в нем пароли с помощью следующих параметров:

   - `ZABBIX_DB_SECRET` – Root-пароль базы данных системы мониторинга Zabbix.
   - `MONGO_ADMIN_SECRET` – пароль администратора базы данных MongoDB.
   - `MONGO_USER_SECRET` – пароль пользователя базы данных MongoDB. Этот пароль используется оркестратором.
   - `CTL_CERT_SECRET` – пароль SSL-сертификата контроллера.
   - `ORC_CERT_SECRET` – пароль SSL-сертификата оркестратора.
   - `ORC_ENC_SECRET` – пароль для шифрования конфиденциальных данных в базе данных MongoDB. Минимальная длина: 32 символа.
   - `VNFM_CERT_SECRET` – пароль SSL-сертификата VNFM.

   > Мы рекомендуем убедиться, что длина всех паролей, кроме пароля, указанного с помощью параметра `ORC_ENC_SECRET`, составляет хотя бы 16 символов.

3. Создайте файл vault_password.txt и укажите в нем мастер-пароль.

4. Зашифруйте файл keystore.yml:

   - Если вы хотите зашифровать файл keystore.yml в режиме attended, выполните команду:

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

   - Если вы хотите зашифровать файл keystore.yml в режиме unattended, выполните команду:

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

Пароли будут сгенерированы и зашифрованы.

Изменение паролей

Чтобы изменить пароли:

1. Расшифруйте файл keystore.yml:

   - Если вы хотите расшифровать файл keystore.yml в режиме attended, выполните команду:

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

   - Если вы хотите расшифровать файл keystore.yml в режиме unattended, выполните команду:

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

2. Измените следующие пароли в файле keystore.yml:

   - `ZABBIX_DB_SECRET` – Root-пароль базы данных системы мониторинга Zabbix.
   - `MONGO_ADMIN_SECRET` – пароль администратора базы данных MongoDB.
   - `MONGO_USER_SECRET` – пароль пользователя базы данных MongoDB. Этот пароль используется оркестратором.
   - `CTL_CERT_SECRET` – пароль SSL-сертификата контроллера.
   - `ORC_CERT_SECRET` – пароль SSL-сертификата оркестратора.
   - `ORC_ENC_SECRET` – пароль для шифрования конфиденциальных данных в базе данных MongoDB. Минимальная длина: 32 символа.
   - `VNFM_CERT_SECRET` – пароль SSL-сертификата VNFM.

   > Мы рекомендуем убедиться, что длина всех паролей, кроме пароля, указанного с помощью параметра `ORC_ENC_SECRET`, составляет хотя бы 16 символов.

3. Зашифруйте файл keystore.yml:

   - Если вы хотите зашифровать файл keystore.yml в режиме attended, выполните команду:

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

   - Если вы хотите зашифровать файл keystore.yml в режиме unattended, выполните команду:

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

Пароли будут изменены и зашифрованы.

Настройка конфигурационного файла

Вам нужно указать параметры развертывания Kaspersky SD-WAN в конфигурационном файле в формате YAML на устройстве администратора. Путь к конфигурационному файлу необходимо указать при развертывании решения. Вы можете использовать примеры конфигурационных файлов для типовых схем развертывания, которые содержатся в директориях inventory/external/pnf и inventory/external/vnf архива установки.

Конфигурационный файл состоит из двух основных блоков:

- `nodes` – виртуальные машины или физические серверы для развертывания компонентов Kaspersky SD-WAN. При развертывании решения на виртуальных машинах или физических серверах автоматически генерируются правила iptables для взаимодействия компонентов решения друг с другом.
- `external` – параметры развертывания Kaspersky SD-WAN.

Мы не рекомендуем изменять значения параметров по умолчанию.

Блок `nodes` имеет следующую структуру:

Блок/параметр			Описание
`node_< номер виртуальной машины или физического сервера >`			Параметры развертывания виртуальной машины или физического сервера.
	`ip`		IP-адрес виртуальной машины или физического сервера. Вам нужно ввести значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126`
	`vip`		Виртуальный IP-адрес виртуальной машины или физического сервера. Вам нужно ввести значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` Этот параметр необходимо указать для всех виртуальных машин или физических серверов, на которых вы планируете использовать виртуальные IP-адреса.
	`knaas_aio_int`		Параметры подключения Docker-контейнеров компонентов Kaspersky SD-WAN к локальной виртуальной сети виртуальной машины или физического сервера.
		`base`	Первые три октета IP-адреса локальной виртуальной сети. Значение по умолчанию: `10.11.11`. Вам нужно ввести значение в формате `XXX.XXX.XXX`, например: `192.168.110` Вы можете изменить первые три октета IP-адреса по умолчанию, если они пересекаются с вашим адресным пространством.
		`mode`	Режим работы локальной виртуальной сети. Возможные значения: • `bridge` – на виртуальной машине или физическом сервере создается Linux-мост. Docker-контейнеры подключаются к Linux-мосту по L3-сети с помощью NAT и iptables. • `vlan` – Docker-контейнеры подключаются к интерфейсу виртуальной машины или физического сервера по L2-сети с помощью macvlan-драйвера. Мы рекомендуем указывать это значение только при использовании доверенной L2-сети, так как в этом случае на виртуальной машине или физическом сервере не используется межсетевой экран.
		`iface`	Имя интерфейса виртуальной машины или физического сервера для подключения Docker-контейнеров по L2-сети, например: `enp6s0` Этот параметр необходимо указать, если для параметра `mode` вы указали значение `vlan`.
		`vlan`	VLAN-тег L2-сети. Вам нужно ввести значение в диапазоне от 1 до 4095. Если вы не хотите использовать VLAN-тег, введите `0`. Этот параметр необходимо указать, если для параметра `mode` вы указали значение `vlan`.
	`knaas_os_man`		Параметры подключения Docker-контейнеров компонентов Kaspersky SD-WAN к управляющей виртуальной сети виртуальной машины или физического сервера.
		`base`	Первые три октета IP-адреса управляющей виртуальной сети. Значение по умолчанию: `10.11.11`. Вам нужно ввести значение в формате `XXX.XXX.XXX`, например: `192.168.110` Вы можете изменить первые три октета IP-адреса по умолчанию, если они пересекаются с вашим адресным пространством.
		`mode`	Режим работы управляющей виртуальной сети. Возможные значения: • `bridge` – на виртуальной машине или физическом сервере создается Linux-мост. Docker-контейнеры подключаются к Linux-мосту по L3-сети с помощью NAT и iptables. • `vlan` – Docker-контейнеры подключаются к интерфейсу виртуальной машины или физического сервера по L2-сети с помощью macvlan-драйвера. Мы рекомендуем указывать это значение только при использовании доверенной L2-сети, так как в этом случае на виртуальной машине или физическом сервере не используется межсетевой экран.
		`iface`	Имя интерфейса виртуальной машины или физического сервера для подключения Docker-контейнеров по L2-сети, например: `enp6s0` Этот параметр необходимо указать, если для параметра `mode` вы указали значение `vlan`.
		`vlan`	VLAN-тег L2-сети. Вам нужно ввести значение в диапазоне от 1 до 4095. Если вы не хотите использовать VLAN-тег, введите `0`. Этот параметр необходимо указать, если для параметра `mode` вы указали значение `vlan`.

Блок `external` имеет следующую структуру:

Блок/параметр			Описание
`vault_passwords_dirname`			Путь к директории /passwords на устройстве администратора со сгенерированными вручную паролями. Если вы не генерируете пароли вручную, они автоматически генерируются при развертывании решения и помещаются в директорию /passwords распакованного архива установки на устройстве администратора.
`ansible_user`			Имя учетной записи на устройстве администратора и виртуальных машинах или физических серверах для запуска плейбуков при развертывании решения.
`ssl`			Параметры SSL-сертификатов компонентов Kaspersky SD-WAN.
	`san_list`		Информация, которая добавляется в SSL-сертификаты.

		`ip`	IP-адреса, которые добавляются в SSL-сертификаты. Вам нужно указать список значений в формате `XXX.XXX.XXX.XXX`, например:
			`ip:`
			`- 192.168.2.0`
			`- 192.168.2.1`

		`dns`	Доменные имена, которые добавляются в SSL-сертификаты. Вам нужно указать список значений, например:
			`dns:`
			`- sdwan.kaspersky.com`
			`- kaspersky.sdwan.com`

	`path_local`		Путь к директории на устройстве администратора со сгенерированными вручную SSL-сертификатами. Если вы не генерируете SSL-сертификаты вручную, они автоматически генерируются при развертывании решения и помещаются в директорию /ssl распакованного архива установки на устройстве администратора.
	`path_remote`		Путь к директории на виртуальных машинах или физических серверах со сгенерированными вручную SSL-сертификатами. Если вы не генерируете SSL-сертификаты вручную, они автоматически генерируются при развертывании решения и помещаются в директорию /ssl на виртуальных машинах или физических серверах.
`syslog`			Параметры syslog-сервера.
	`docker_memory_limit`		Объем оперативной памяти в мегабайтах для Docker-контейнеров syslog-сервера.
	`max_log_size`		Объем оперативной памяти в гигабайтах для журналов syslog-сервера.
	`state`		Развертывание syslog-сервера на виртуальных машинах или физических серверах. Возможные значения: • `enabled` • `disabled`
`zabbix`			Параметры системы мониторинга Zabbix. Более подробную информацию можно получить из официальной документации решения Zabbix.

syslog_server_address	Веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора отправляют журналы. Значение указывается в формате `< протокол >://< адрес хоста >:< номер порта >.` В качестве адреса хоста можно указать IP-адрес или FQDN хоста.
	Примеры:
	`udp://192.168.2.15:1514`
	`tcp+tls://my-syslog-server:1514`
	Если для переменной `secure_syslog` указано `true`, в качестве префикса протокола необходимо указать `tcp+tls`, например:
	`tcp+tls://192.168.2.15:1514`
	Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите адрес хоста в формате FQDN.
	Параметры syslog-сервера можно указать в блоке `syslog`.

secure_syslog	Определяет необходимость шифрования сообщений syslog, отправляемых Docker-контейнером. Возможные значения: • `true` • `false` Значение по умолчанию: `false`. Если указано `false`, сообщения syslog будут оправляться по UDP в незашифрованном виде. Если указано `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат сервера syslog, в переменной `syslog_server_ca_cert_file_path`.
syslog_server_ca_cert_file_path	Абсолютный путь к файлу CA-сертификата, которым подписан сертификат сервера syslog. Обязательный параметр, если для переменной `secure_syslog` указано `true`.
syslog_format	Формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения: `rfc3164` – формат, совместимый с RFC 3164. `rfc5424` – формат, совместимый с RFC 5424. `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд. Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.
db_docker_memory_limit	Объем оперативной памяти в мегабайтах для Docker-контейнеров базы данных системы мониторинга Zabbix.
srv_docker_memory_limit	Объем оперативной памяти в мегабайтах для Docker-контейнеров сервера Zabbix.
www_docker_memory_limit	Объем оперативной памяти в мегабайтах для Docker-контейнеров frontend-части системы мониторинга Zabbix.
proxy_docker_memory_limit	Объем оперативной памяти в мегабайтах для Docker-контейнеров сервера Zabbix-прокси.
cachesize	Объем оперативной памяти в гигабайтах для кеша системы мониторинга Zabbix. Вам нужно ввести значение в формате `< количество гигабайт >G,` например: `8G`
zabbix_<1-3>	Параметры развертывания узлов системы мониторинга Zabbix. Вы можете развернуть один узел системы мониторинга Zabbix без высокой доступности (англ. high availability) или три узла с высокой доступностью.

		`ansible_host`	IP-адрес виртуальной машины или физического сервера из блока `nodes` для развертывания системы мониторинга Zabbix. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` • Переменная Ansible, например: `{{ nodes.node_1.ip }}`
		`db`	Параметры развертывания базы данных системы мониторинга Zabbix.
		`inventory_hostname`	Имя хоста базы данных системы мониторинга Zabbix. Значение по умолчанию: `zabbix-db-<1-3>`.
		`state`	Развертывание базы данных системы мониторинга Zabbix на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
		`srv`	Параметры развертывания сервера Zabbix. При развертывании трех узлов системы мониторинга Zabbix вам нужно указать эти параметры только для двух узлов.
		`inventory_hostname`	Имя хоста сервера Zabbix. Значение по умолчанию: `zabbix-srv-<1-3>`.
		`state`	Развертывание сервера Zabbix на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
		`www`	Параметры развертывания frontend-части системы мониторинга Zabbix. При развертывании трех узлов системы мониторинга Zabbix вам нужно указать эти параметры только для двух узлов.
		`inventory_hostname`	Имя хоста frontend-части системы мониторинга Zabbix. Значение по умолчанию: `zabbix-www-<1-3>`.
		`state`	Развертывание frontend-части системы мониторинга Zabbix на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
		`proxy`	Параметры развертывания сервера Zabbix-прокси. При развертывании трех узлов системы мониторинга Zabbix вам нужно указать эти параметры только для двух узлов.
		`inventory_hostname`	Имя хоста сервера Zabbix-прокси. Значение по умолчанию: `zabbix-proxy-<1-3>`.
		`state`	Развертывание сервера Zabbix-прокси на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
`mongo`			Параметры базы данных MongoDB. Более подробную информацию можно получить из официальной документации базы данных MongoDB.

	`syslog_server_address`		Веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора отправляют журналы. Значение указывается в формате `< протокол >://< адрес хоста >:< номер порта >.` В качестве адреса хоста можно указать IP-адрес или FQDN хоста.
			Примеры:
			`udp://192.168.2.15:1514`
			`tcp+tls://my-syslog-server:1514`
			Если для переменной `secure_syslog` указано `true`, в качестве префикса протокола необходимо указать `tcp+tls`, например:
			`tcp+tls://192.168.2.15:1514`
			Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите адрес хоста в формате FQDN.
			Параметры syslog-сервера можно указать в блоке `syslog`.

	`secure_syslog`		Определяет необходимость шифрования сообщений syslog, отправляемых Docker-контейнером. Возможные значения: • `true` • `false` Значение по умолчанию: `false`. Если указано `false`, сообщения syslog будут оправляться по UDP в незашифрованном виде. Если указано `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат сервера syslog, в переменной `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`		Абсолютный путь к файлу CA-сертификата, которым подписан сертификат сервера syslog. Обязательный параметр, если для переменной `secure_syslog` указано `true`.
	`syslog_format`		Формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения: `rfc3164` – формат, совместимый с RFC 3164. `rfc5424` – формат, совместимый с RFC 5424. `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд. Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.
	`docker_memory_limit`		Объем оперативной памяти в мегабайтах для Docker-контейнеров базы данных MongoDB.
	`mongo_<1-3>`		Параметры развертывания узлов базы данных MongoDB. Вы можете развернуть один узел базы данных MongoDB без высокой доступности или три узла с высокой доступностью. Если вы развертываете три узла базы данных MongoDB, последний узел становится узлом-арбитром.
		`inventory_hostname`	Имя хоста базы данных MongoDB. Значение по умолчанию: `mongo-<1-3>`
		`state`	Развертывание базы данных MongoDB на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
		`ansible_host`	IP-адрес виртуальной машины или физического сервера из блока `nodes` для развертывания базы данных MongoDB. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` • Переменная Ansible, например: `{{ nodes.node_1.ip }}`
`redis`			Параметры базы данных Redis. Более подробную информацию можно получить из официальной документации базы данных Redis.

	`syslog_server_address`	Веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора отправляют журналы. Значение указывается в формате `< протокол >://< адрес хоста >:< номер порта >`. В качестве адреса хоста можно указать IP-адрес или FQDN хоста.
		Примеры:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Если для переменной `secure_syslog` указано `true`, в качестве префикса протокола необходимо указать `tcp+tls`, например:
		`tcp+tls://192.168.2.15:1514`
		Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите адрес хоста в формате FQDN.
		Параметры syslog-сервера можно указать в блоке `syslog`.

	`secure_syslog`	Определяет необходимость шифрования сообщений syslog, отправляемых Docker-контейнером. Возможные значения: • `true` • `false` Значение по умолчанию: `false`. Если указано `false`, сообщения syslog будут оправляться по UDP в незашифрованном виде. Если указано `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат сервера syslog, в переменной `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`	Абсолютный путь к файлу CA-сертификата, которым подписан сертификат сервера syslog. Обязательный параметр, если для переменной `secure_syslog` указано `true`.
	`syslog_format`	Формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения: `rfc3164` – формат, совместимый с RFC 3164. `rfc5424` – формат, совместимый с RFC 5424. `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд. Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.
	`docker_memory_limit`	Объем оперативной памяти в мегабайтах для Docker-контейнеров базы данных Redis.
	`redis_<1-3>m`	Параметры развертывания узлов сервера Redis replica. Вы можете развернуть один узел сервера Redis replica без высокой доступности или три узла с высокой доступностью.
	`inventory_hostname`	Имя хоста сервера Redis replica. Значение по умолчанию: `redis-<1-3>m`.
	`state`	Развертывание сервера Redis replica на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
	`ansible_host`	IP-адрес виртуальной машины или физического сервера из блока `nodes` для развертывания сервера Redis replica. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` • Переменная Ansible, например: `{{ nodes.node_1.ip }}`
	`redis_<1-3>s`	Параметры развертывания узлов системы Redis Sentinel. Если вы развертываете три узла сервера Redis replica с высокой доступностью, вам также нужно развернуть три узла системы Redis Sentinel.

		`inventory_hostname`	Имя хоста системы Redis Sentinel. Значение по умолчанию: `redis-<1-3>s`.
		`state`	Развертывание системы Redis Sentinel на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
		`ansible_host`	IP-адрес виртуальной машины или физического сервера из блока `nodes` для развертывания системы Redis Sentinel. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` • Переменная Ansible, например: `{{ nodes.node_1.ip }}`
`ctl`			Параметры развертывания контроллера. Вам нужно развернуть контроллер в виде физической сетевой функции, чтобы развернуть экземпляр SD-WAN для тенанта. Вместе с каждым узлом контроллера на виртуальной машине или физическом сервере автоматически разворачивается компонент MOCKPNF для обеспечения безопасности настройки Docker-контейнера узла контроллера.

`tenants`			Параметры тенантов, для которых вы развертываете экземпляры SD-WAN.
`- name`			Имя тенанта.
	`state`		Создание тенанта и развертывание контроллера на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
	`ctl_base`		Первые три октета IP-адреса виртуальной сети контроллера. Вам нужно ввести значение в формате `XXX.XXX.XXX`, например: `192.168.110` При развертывании демонстрационного стенда Kaspersky SD-WAN в соответствии со схемой развертывания все-в-одном значение этого параметра может совпадать со значением параметра `base` в блоке `nodes`.
	`mock_base`		Первые три октета IP-адреса управляющей виртуальной сети контроллера. Вам нужно ввести значение в формате `XXX.XXX.XXX`, например: `192.168.110`
	`hosts`		Параметры развертывания контроллера. Вы можете развернуть один узел контроллера без высокой доступности, либо три или пять узлов с высокой доступностью. Если вы развертываете три или пять узлов контроллера, последний узел становится узлом-арбитром.
	`- inventory_hostname`		Имя хоста узла контроллера. Значение по умолчанию: `ctl-<1-5>`.
		`ansible_host`	IP-адрес виртуальной машины или физического сервера из блока `nodes` для развертывания узла контроллера. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` • Переменная Ansible, например: `{{ nodes.node_1.ip }}`
	`docker_memory_limit`		Объем оперативной памяти в мегабайтах для Docker-контейнеров контроллера.
	`JAVA_OPTS`		Параметры оперативной памяти виртуальной машины Java.
		`Xms`	Минимальный объем heap-памяти, который виртуальная машина Java может назначить контроллеру. Вам нужно ввести значение в одном из следующих форматов: • `< объем памяти >m` – объем памяти в мегабайтах, например: `512m` • `< объем памяти >g` – объем памяти в гигабайтах, например: `2g` Мы рекомендуем указать для этого параметра значение, которое вдвое меньше значения параметра `Xmx`.
		`Xmx`	Максимальный объем heap-памяти, который виртуальная машина Java может назначить контроллеру. Вам нужно ввести значение в одном из следующих форматов: • `< объем памяти >m` – объем памяти в мегабайтах, например: `512m` • `< объем памяти >g` – объем памяти в гигабайтах, например: `4g` Мы рекомендуем указать для этого параметра значение, которое вдвое меньше значения параметра `docker_memory_limit`.
		`MaxDirectMemorySize`	Максимальный объем прямой памяти (англ. direct memory), который виртуальная машина Java может назначить контроллеру. Вам нужно ввести значение в одном из следующих форматов: • `< объем памяти >m` – объем памяти в мегабайтах, например: `512m` • `< объем памяти >g` – объем памяти в гигабайтах, например: `4g` Мы рекомендуем указать для этого параметра значение, которое вдвое меньше значения параметра `docker_memory_limit`.

	`syslog_server_address`	Веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора отправляют журналы. Значение указывается в формате `< протокол >://< адрес хоста >:< номер порта >.` В качестве адреса хоста можно указать IP-адрес или FQDN хоста.
		Примеры:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Если для переменной `secure_syslog` указано `true`, в качестве префикса протокола необходимо указать `tcp+tls`, например:
		`tcp+tls://192.168.2.15:1514`
		Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите адрес хоста в формате FQDN.
		Параметры syslog-сервера можно указать в блоке `syslog`.

	`secure_syslog`	Определяет необходимость шифрования сообщений syslog, отправляемых Docker-контейнером. Возможные значения: • `true` • `false` Значение по умолчанию: `false`. Если указано `false`, сообщения syslog будут оправляться по UDP в незашифрованном виде. Если указано `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат сервера syslog, в переменной `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`	Абсолютный путь к файлу CA-сертификата, которым подписан сертификат сервера syslog. Обязательный параметр, если для переменной `secure_syslog` указано `true`.
	`syslog_format`	Формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения: `rfc3164` – формат, совместимый с RFC 3164. `rfc5424` – формат, совместимый с RFC 5424. `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд. Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.
`www`		Параметры frontend-части решения.

	`syslog_server_address`	Веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора отправляют журналы. Значение указывается в формате `< протокол >://< адрес хоста >:< номер порта >.` В качестве адреса хоста можно указать IP-адрес или FQDN хоста.
		Примеры:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Если для переменной `secure_syslog` указано `true`, в качестве префикса протокола необходимо указать `tcp+tls`, например:
		`tcp+tls://192.168.2.15:1514`
		Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите адрес хоста в формате FQDN.
		Параметры syslog-сервера можно указать в блоке `syslog`.

	`secure_syslog`	Определяет необходимость шифрования сообщений syslog, отправляемых Docker-контейнером. Возможные значения: • `true` • `false` Значение по умолчанию: `false`. Если указано `false`, сообщения syslog будут оправляться по UDP в незашифрованном виде. Если указано `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат сервера syslog, в переменной `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`	Абсолютный путь к файлу CA-сертификата, которым подписан сертификат сервера syslog. Обязательный параметр, если для переменной `secure_syslog` указано `true`.
	`syslog_format`	Формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения: `rfc3164` – формат, совместимый с RFC 3164. `rfc5424` – формат, совместимый с RFC 5424. `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд. Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.
	`docker_memory_limit`	Объем оперативной памяти в мегабайтах для Docker-контейнеров frontend-части решения.
	`oem`	Параметры отображения графических элементов веб-интерфейса оркестратора. С помощью этого блока вы можете изменить графические элементы веб-интерфейса оркестратора.

		`state`	Изменение графических элементов по умолчанию веб-интерфейса оркестратора. Возможные значения: • `enabled` • `disabled`
		`path_local`	Путь к директории на устройстве администратора с графическими элементами веб-интерфейса оркестратора. Графические элементы по умолчанию веб-интерфейса оркестратора содержатся в директории /oem распакованного архива установки на устройстве администратора.
		`path_remote`	Путь к директории на виртуальных машинах или физических серверах с графическими элементами веб-интерфейса оркестратора.
		`title`	Название, которое которое отображается на фоне при входе в веб-интерфейс оркестратора. Значение по умолчанию: `Kaspersky SD-WAN`. Рекомендуемая длина: не более 128 символов.
		`support`	Веб-адрес, который отображается в нижней части веб-интерфейса оркестратора. Значение по умолчанию: `support.kaspersky.com`. Рекомендуемая длина: не более 128 символов.
		`assets`	Замена графических элементов по умолчанию веб-интерфейса оркестратора на графические элементы, которые вы поместили в директорию на устройстве администратора. Возможные значения: • `enabled` • `disabled` Вам нужно указать директорию на устройстве администратора с графическими элементами веб-интерфейса оркестратора с помощью параметра `path_local`.
	`www_<1-2>`		Параметры развертывания узлов frontend-части решения. Вы можете развернуть один узел frontend-части решения без высокой доступности или два узла с высокой доступностью. Вам нужно развернуть узлы frontend-части решения и узлы оркестратора на одних виртуальных машинах или физических серверах. Например, первый узел frontend-части решения необходимо развернуть на одной виртуальной машине или физическом сервере с первым узлом оркестратора. Параметры оркестратора можно указать в блоке `orc`.
		`inventory_hostname`	Имя хоста frontend-части решения. Значение по умолчанию: `www-<1-2>`.
		`state`	Развертывание frontend-части решения на виртуальной машине или физическом сервере. Возможные значения: • `enabled`; • `disabled`.
		`ansible_host`	IP-адрес виртуальной машины или физического сервера из блока `nodes` для развертывания frontend-части решения. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` • Переменная Ansible, например: `{{ nodes.node_1.ip }}`
`orc`			Параметры оркестратора.

`syslog_server_address`		Веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора отправляют журналы. Значение указывается в формате `< протокол >://< адрес хоста >:< номер порта >.` В качестве адреса хоста можно указать IP-адрес или FQDN хоста.
		Примеры:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Если для переменной `secure_syslog` указано `true`, в качестве префикса протокола необходимо указать `tcp+tls`, например:
		`tcp+tls://192.168.2.15:1514`
		Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите адрес хоста в формате FQDN.
		Параметры syslog-сервера можно указать в блоке `syslog`.

`secure_syslog`		Определяет необходимость шифрования сообщений syslog, отправляемых Docker-контейнером. Возможные значения: • `true` • `false` Значение по умолчанию: `false`. Если указано `false`, сообщения syslog будут оправляться по UDP в незашифрованном виде. Если указано `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат сервера syslog, в переменной `syslog_server_ca_cert_file_path`.
`syslog_server_ca_cert_file_path`		Абсолютный путь к файлу CA-сертификата, которым подписан сертификат сервера syslog. Обязательный параметр, если для переменной `secure_syslog` указано `true`.
`syslog_format`		Формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения: `rfc3164` – формат, совместимый с RFC 3164. `rfc5424` – формат, совместимый с RFC 5424. `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд. Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.
`docker_memory_limit`		Объем оперативной памяти в мегабайтах для Docker-контейнеров оркестратора.
`JAVA_OPTS`		Параметры оперативной памяти виртуальной машины Java.
	`Xms`	Минимальный объем heap-памяти, который виртуальная машина Java может назначить оркестратору. Вам нужно ввести значение в одном из следующих форматов: • `< объем памяти >m` – объем памяти в мегабайтах, например: `512m` • `< объем памяти >g` – объем памяти в гигабайтах, например: `4g` Мы рекомендуем указать для этого параметра значение, которое вдвое меньше значения параметра `Xmx`.
	`Xmx`	Максимальный объем heap-памяти, который виртуальная машина Java может назначить оркестратору. Вам нужно ввести значение в одном из следующих форматов: • `< объем памяти >m` – объем памяти в мегабайтах, например: `512m` • `< объем памяти >g` – объем памяти в гигабайтах, например: `4g` Мы рекомендуем указать для этого параметра значение, которое вдвое меньше значения параметра `docker_memory_limit`.

	number_of_containers		Количество экземпляров контейнеров оркестратора для балансировки нагрузки. Диапазон значений: `1 – 5`. Если параметр отсутствует, используется значение по умолчанию (`1`). Значение параметра игнорируется, если в параметре `ansible_host` для блоков `orc_1` и `orc_2` указан массив и количество элементов в нем больше одного.
	orc_<1-2>		Параметры развертывания узлов оркестратора. Вы можете развернуть один узел оркестратора без высокой доступности или два узла с высокой доступностью. Вам нужно развернуть узлы оркестратора и узлы frontend-части решения на одних виртуальных машинах или физических серверах. Например, первый узел оркестратора необходимо развернуть на одной виртуальной машине или физическом сервере с первым узлом frontend-части решения. Параметры frontend-части решения можно указать в блоке `www`.
		inventory_hostname	Имя хоста оркестратора. Значение по умолчанию: `orc-<1-2>`.
		state	Развертывание оркестратора на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`

		ansible_host	IP-адреса узлов (виртуальных машин или физических серверов) из блока `nodes` для развертывания оркестратора. Возможно указание как одного IP-адреса в виде строки, так и списка IP-адресов в виде массива строк. Значение IP-адреса может указываться в виде строки в формате `XXX.XXX.XXX.XXX` либо в виде переменной Ansible.
			Примеры:
			• Строка в формате `XXX.XXX.XXX.XXX`:
			`192.168.110.126`
			• Переменная Ansible:
			`{{ nodes.node_1.ip }}`
			• Массив переменных Ansible:
			`{{ [nodes.node_1.ip, nodes.node_2.ip, nodes.node_3.ip, nodes.node_4.ip, nodes.node_5.ip] }}`
			Если указан массив, то параметр `number_of_containers` игнорируется, и балансировка нагрузки между экземплярами оркестратора достигается за счет вынесения контейнеров оркестратора на отдельные узлы, указанные в массиве.

vnfm			Параметры менеджера виртуальных сетевых функций.

`syslog_server_address`		Веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора отправляют журналы. Значение указывается в формате `< протокол >://< адрес хоста >:< номер порта >.` В качестве адреса хоста можно указать IP-адрес или FQDN хоста.
		Примеры:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Если для переменной `secure_syslog` указано `true`, в качестве префикса протокола необходимо указать `tcp+tls`, например:
		`tcp+tls://192.168.2.15:1514`
		Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите адрес хоста в формате FQDN.
		Параметры syslog-сервера можно указать в блоке `syslog`.

`secure_syslog`		Определяет необходимость шифрования сообщений syslog, отправляемых Docker-контейнером. Возможные значения: • `true` • `false` Значение по умолчанию: `false`. Если указано `false`, сообщения syslog будут оправляться по UDP в незашифрованном виде. Если указано `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат сервера syslog, в переменной `syslog_server_ca_cert_file_path`.
`syslog_server_ca_cert_file_path`		Абсолютный путь к файлу CA-сертификата, которым подписан сертификат сервера syslog. Обязательный параметр, если для переменной `secure_syslog` указано `true`.
`syslog_format`		Формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения: `rfc3164` – формат, совместимый с RFC 3164. `rfc5424` – формат, совместимый с RFC 5424. `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд. Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.
`docker_memory_limit`		Объем оперативной памяти в мегабайтах для Docker-контейнеров оркестратора.
`JAVA_OPTS`		Параметры оперативной памяти виртуальной машины Java.
	`Xms`	Минимальный объем heap-памяти, который виртуальная машина Java может назначить менеджеру виртуальных сетевых функций. Вам нужно ввести значение в одном из следующих форматов: • `< объем памяти >m` – объем памяти в мегабайтах, например: `512m` • `< объем памяти >g` – объем памяти в гигабайтах, например: `4g` Мы рекомендуем указать для этого параметра значение, которое вдвое меньше значения параметра `Xmx`.
	`Xmx`	Максимальный объем heap-памяти, который виртуальная машина Java может назначить менеджеру виртуальных сетевых функций. Вам нужно ввести значение в одном из следующих форматов: • `<объем памяти>m` – объем памяти в мегабайтах, например: `512m` • `<объем памяти>g` – объем памяти в гигабайтах, например: `4g` Мы рекомендуем указать для этого параметра значение, которое вдвое меньше значения параметра `docker_memory_limit`.
`vnfm_<1-2>`		Параметры развертывания узлов менеджера виртуальных сетевых функций. Вы можете развернуть один узел менеджера виртуальных сетевых функций без высокой доступности или два узла с высокой доступностью.

		`inventory_hostname`	Имя хоста менеджера виртуальных сетевых функций. Значение по умолчанию: `vnfm-<1-2>`.
		`state`	Развертывание менеджера виртуальных сетевых функций на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
		`ansible_host`	IP-адрес виртуальной машины или физического сервера из блока `nodes` для развертывания менеджера виртуальных сетевых функций. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` • Переменная Ansible, например: `{{ nodes.node_1.ip }}`
`vnfm_proxy`			Параметры прокси-менеджера виртуальных сетевых функций.

	`syslog_server_address`	Веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора отправляют журналы. Значение указывается в формате `< протокол >://< адрес хоста >:< номер порта >.` В качестве адреса хоста можно указать IP-адрес или FQDN хоста.
		Примеры:
		`udp://192.168.2.15:1514`
		`tcp+tls://my-syslog-server:1514`
		Если для переменной `secure_syslog` указано `true`, в качестве префикса протокола необходимо указать `tcp+tls`, например:
		`tcp+tls://192.168.2.15:1514`
		Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите адрес хоста в формате FQDN.
		Параметры syslog-сервера можно указать в блоке `syslog`.

	`secure_syslog`	Определяет необходимость шифрования сообщений syslog, отправляемых Docker-контейнером. Возможные значения: • `true` • `false` Значение по умолчанию: `false`. Если указано `false`, сообщения syslog будут оправляться по UDP в незашифрованном виде. Если указано `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат сервера syslog, в переменной `syslog_server_ca_cert_file_path`.
	`syslog_server_ca_cert_file_path`	Абсолютный путь к файлу CA-сертификата, которым подписан сертификат сервера syslog. Обязательный параметр, если для переменной `secure_syslog` указано `true`.
	`syslog_format`	Формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения: `rfc3164` – формат, совместимый с RFC 3164. `rfc5424` – формат, совместимый с RFC 5424. `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд. Если в качестве сервера syslog вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.
	`docker_memory_limit`	Объем оперативной памяти в мегабайтах для Docker-контейнеров прокси-менеджера виртуальных сетевых функций.
	`vnfm_proxy_<1-2>`	Параметры развертывания узлов прокси-менеджера виртуальных сетевых функций. Вы можете развернуть один узел прокси-менеджера виртуальных сетевых функций без высокой доступности или два узла с высокой доступностью.
	`inventory_hostname`	Имя хоста прокси-менеджера виртуальных сетевых функций. Значение по умолчанию: `vnfm-proxy-<1-2>`.
	`state`	Развертывание прокси-менеджера виртуальных сетевых функций на виртуальной машине или физическом сервере. Возможные значения: • `enabled` • `disabled`
	`ansible_host`	IP-адрес виртуальной машины или физического сервера из блока `nodes` для развертывания прокси-менеджера виртуальных сетевых функций. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` • Переменная Ansible, например: `{{ nodes.node_1.ip }}`

Пример конфигурационного файла

```
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 }}
```

Изменение графических элементов веб-интерфейса оркестратора

Чтобы изменить графические элементы веб-интерфейса оркестратора:

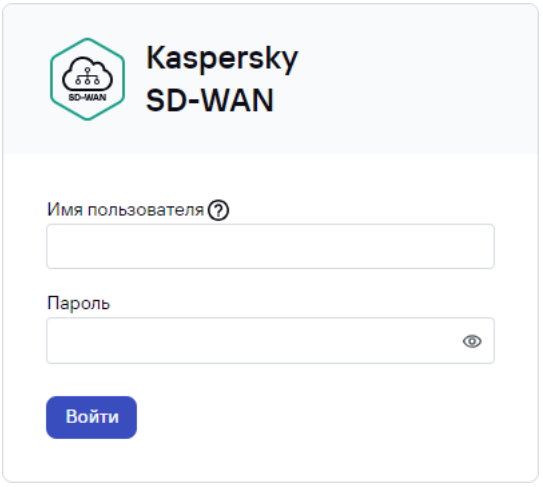
1. Настройте frontend-часть решения в блоке `www` конфигурационного файла.

2. На устройстве администратора перейдите в директорию /oem распакованного архива установки. В этой директории содержатся графические элементы по умолчанию веб-интерфейса оркестратора. Вы можете заменить следующие файлы:

   - favicon.png и favicon.svg - значок, который отображается на вкладке с веб-интерфейсом оркестратора.

   - login_logo.svg – значок, который отображается в верхней части окна при входе в веб-интерфейс оркестратора.

   - logo_activation.svg - значок, который отображается при автоматической регистрации устройства CPE.

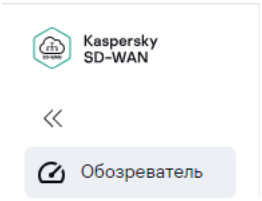


Kaspersky SD-WAN

To apply the configuration to the current KESR click the button below

Apply configuration

- logo.svg и title.svg - значок и название, которые отображаются в верхней части навигационной панели веб-интерфейса оркестратора.



Замена вышедшего из строя узла контроллера

Вы можете развернуть новый узел контроллера для замены узла контроллера, который вышел из строя без возможности восстановления. Если узел контроллера вышел из строя, находясь в кластере с другими узлами, новый узел контроллера будет автоматически добавлен в этот кластер и синхронизирован с существующими узлами.

Перед выполнением этого сценария вам нужно убедиться, что IP-адрес виртуальной машины или физического сервера для развертывания нового узла контроллера совпадает с IP-адресом виртуальной машины или физического сервера, на котором был развернут вышедший из строя узел контроллера. Вы указали IP-адреса виртуальных машин или физических серверов для развертывания узлов контроллера при развертывании решения в блоке `ctl` конфигурационного файла.

Сценарий замены вышедшего из строя узла контроллера состоит из следующих этапов:

1. **Подготовка устройства администратора**

Подготовьте устройство администратора для развертывания нового узла контроллера. Устройство администратора может быть локальной или удаленной виртуальной машиной, а также персональным компьютером. При развертывании демонстрационного стенда Kaspersky SD-WAN в соответствии со схемой развертывания все-в-одном в качестве устройства администратора необходимо использовать виртуальную машину.

2. **Обеспечение сетевой связности между устройством администратора, компонентами решения и новым узлом контроллера**

   Обеспечьте сетевую связность между устройством администратора, компонентами решения и виртуальной машиной или физическим сервером, на котором вы хотите развернуть новый узел контроллера. Вам нужно убедиться, что каналы связи между виртуальными машинами или физическими серверами соответствуют аппаратным и программным требованиям.

   > Виртуальную машину или физический сервер необходимо развернуть в доверенном сетевом сегменте, чтобы избежать компрометации передаваемого трафика.

3. **Развертывание узла контроллера**

   Выполните следующие действия на устройстве администратора:

   1. Примите Лицензионное соглашение, выполнив команду:

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

   2. Перейдите в распакованный архив установки.

   3. Если вы хотите развернуть новый узел контроллера в режиме attended, выполните одно из следующих действий:

      - Если при развертывании решения вы сгенерировали вручную пароли, выполните команду:

        ```
        ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
        "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
        ```

        При выполнении команды введите пароль учетной записи root и сгенерированный мастер-пароль.

      - Если при развертывании решения вы не сгенерировали вручную пароли, выполните команду:

        ```
        ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
        "@inventory/external/images.yml" -K knaas/knaas-install.yml
        ```

   4. Если вы хотите развернуть новый узел контроллера в режиме unattended, выполните одно из следующих действий:

      > Мы рекомендуем использовать этот режим только в доверенной среде, так как в противном случае злоумышленники могут перехватить ваши пароли.

      - Если при развертывании решения вы сгенерировали вручную пароли, выполните команду:

        ```
        ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
        "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --
        vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
        ```

      - Если при развертывании решения вы не сгенерировали вручную пароли, выполните команду:

        ```
        ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
        "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword"
        knaas/knaas-install.yml
        ```

Новый узел контроллера будет развернут вместо вышедшего из строя узла контроллера. Сообщение об успешном развертывании отобразится в консоли устройства администратора.

Если при развертывании узла контроллера возникает проблема сетевой связности с виртуальной машиной или физическим сервером, в консоли устройства администратора отображается ошибка и новый узел контроллера не развертывается. В этом случае вам нужно восстановить сетевую связность, очистить виртуальную машину или физический сервер, после чего заново выполнить команду развертывания.

Обновление Kaspersky SD-WAN

ФУНКЦИОНАЛЬНОСТЬ ОБНОВЛЕНИЙ (ВКЛЮЧАЯ ОБНОВЛЕНИЯ АНТИВИРУСНЫХ СИГНАТУР И ОБНОВЛЕНИЯ КОДОВОЙ БАЗЫ), А ТАКЖЕ ФУНКЦИОНАЛЬНОСТЬ KSN МОГУТ БЫТЬ НЕДОСТУПНЫ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ НА ТЕРРИТОРИИ США.

Перед обновлением Kaspersky SD-WAN вам нужно убедиться, что ни одно из устройств CPE не имеет статус **Ошибка**. Вы можете посмотреть статус устройств CPE в таблице устройств CPE. Также мы рекомендуем сделать резервные копии компонентов решения:

- Если вы развернули компоненты решения на виртуальных машинах, вам нужно сделать снимки мгновенного состояния (англ. snapshots) виртуальных машин. После обновления Kaspersky SD-WAN снимки мгновенного состояния виртуальных машин можно удалить. Более подробную информацию о том, как сделать снимки мгновенного состояния виртуальных машин, можно получить из официальной документации сред виртуализации, с помощью которых вы развернули виртуальные машины.

- Если вы развернули компоненты решения на физических серверах, вам нужно сделать резервные копии жестких дисков физических серверов. При использовании RAID-контроллера (Redundant Array of Independent Disks) информацию о том, как сделать резервные копии жестких дисков вы можете получить из официальной документации производителя RAID-контроллера.

Сценарий обновления Kaspersky SD-WAN состоит из следующих этапов:

1. **Подготовка устройства администратора**

   Подготовьте устройство администратора для обновления решения. Устройство администратора может быть локальной или удаленной виртуальной машиной, а также персональным компьютером. При развертывании демонстрационного стенда Kaspersky SD-WAN в соответствии со схемой развертывания все-в-одном в качестве устройства администратора необходимо использовать виртуальную машину.

2. **Настройка конфигурационного файла**

   Настройте конфигурационный файл в соответствии с изменениями, которые были внесены в новую версию Kaspersky SD-WAN. Вы можете посмотреть изменения в корневой директории архива установки в файле CHANGELOG.md.

   При обновлении Kaspersky SD-WAN убедитесь, что вы не потеряли файлы с паролями и SSL-сертификатами.

3. **Принятие лицензионного соглашениы**

   Примите Лицензионное соглашение, выполнив команду:

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

4. **Обновление Kaspersky SD-WAN**

   Обновите Kaspersky SD-WAN одним из следующих способов:

   - Если вы хотите обновить решение в режиме attended, выполните команду:

     ```
     ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
     "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
     ```

     При выполнении команды введите пароль учетной записи root на устройстве администратора и сгенерированный мастер-пароль.

   - Если вы хотите обновить решение в режиме partially attended, выполните команду:

     ```
     ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
     "@inventory/external/images.yml" -K --vault-password-file
     ./passwords/vault_password.txt knaas/knaas-install.yml
     ```

     При выполнении команды введите пароль учетной записи root на устройстве администратора.

   - Если вы хотите обновить решение в режиме unattended, выполните команду:

     ```
     ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
     "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --
     vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
     ```

Компоненты Kaspersky SD-WAN будут обновлены на виртуальных машинах или физических серверах, которые вы указали в конфигурационном файле. Сообщение об успешном обновлении отобразится в консоли устройства администратора.

Если при обновлении компонентов решения возникает проблема сетевой связности с одной из виртуальных машин или одним из физических серверов, в консоли устройства администратора отображается ошибка и решение не обновляется. В этом случае вам нужно восстановить сетевую связность, после чего заново выполнить команду обновления.

После обновления решения требуется очистить историю команд Bash.

Удаление Kaspersky SD-WAN

Удаление Kaspersky SD-WAN невозможно отменить.

Чтобы удалить Kaspersky SD-WAN,

1. На устройстве администратора перейдите в распакованный архив установки.
2. Удалите Kaspersky SD-WAN одним из следующих способов:

   - Если вы хотите удалить решение в режиме attended, выполните команду:

     ```
     ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
     "@inventory/external/images.yml" -K knaas/knaas-teardown.yml
     ```

   - Если вы хотите удалить решение в режиме unattended, выполните команду:

     ```
     ansible-playbook -i inventory/generic -e "@< путь к конфигурационному файлу >" -e
     "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword"
     knaas/knaas-teardown.yml
     ```

Компоненты Kaspersky SD-WAN будут удалены с виртуальных машин или физических серверов. Сообщение об успешном удалении отобразится в консоли устройства администратора.

Если при удалении компонентов решения возникает проблема сетевой связности с одной из виртуальных машин или одним из физических серверов, в консоли устройства администратора отображается ошибка и решение не удаляется. В этом случае вам нужно восстановить сетевую связность, после чего заново выполнить команду удаления.

Вход и выход из веб-интерфейса оркестратора

Вход в веб-интерфейс оркестратора

Чтобы войти в веб-интерфейс оркестратора:

1. В адресной строке браузера введите один из следующих IP-адресов:

   - Если вы хотите войти на портал администратора, введите IP-адрес виртуальной машины или физического сервера, на котором вы развернули оркестратор или frontend-часть решения. Вы указали IP-адрес виртуальной машины или физического сервера для развертывания оркестратора и frontend-части решения в блоках `orc_<1-2>` и `www_<1-2>` конфигурационного файла при развертывании решения. Вы также можете ввести виртуальный IP-адрес оркестратора.

   - Если вы хотите войти на портал самообслуживания, введите IP-адрес, который вам предоставил администратор платформы.

2. На открывшейся странице аутентификации введите имя пользователя и пароль. Пароль должен содержать как минимум одну прописную букву латинского алфавита (A–Z), одну строчную букву (a–z), одну цифру и один специальный символ. Длина пароля: от 8 до 50 символов.

3. Нажмите на кнопку **Войти**. Если для учетной записи включена двухфакторная аутентификация, выполните следующие действия:

   a. Отсканируйте отобразившийся QR-код физическим или программным аутентификатором, поддерживающим стандарт RFC 6238.

   b. Введите и подтвердите сгенерированный аутентификатором уникальный код.

После успешной аутентификации откроется раздел или подраздел, который вы установили как страницу по умолчанию.

Выход из веб-интерфейса оркестратора

Чтобы выйти из веб-интерфейса оркестратора:

1. В нижней части меню нажмите на значок выхода.

2. В отобразившемся окне подтверждения нажмите на кнопку **OK**.

Вы выйдете из веб-интерфейса оркестратора.

Лицензирование Kaspersky SD-WAN

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky SD-WAN. При необходимости масштабировать решения вы можете приобрести дополнительные лицензии на программное и аппаратное обеспечение.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу. Текст Лицензионного соглашения на поддерживаемых языках находится в файлах *license <код языка>.rtf*, входящих в комплект поставки Kaspersky SD-WAN.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с Kaspersky SD-WAN.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения. Сделать это можно одним из следующих способов:

- Инициализировать переменную окружения `KNAAS_EULA_AGREED` перед запуском Docker-контейнера Kaspersky SD-WAN:

  ```
  export KNAAS_EULA_AGREED=yes
  ```

  В этом случае при запуске Docker-контейнера Kaspersky SD-WAN нужно передавать переменную окружения KNAAS_EULA_AGREED с помощью опции `-e`:

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

- Инициализировать переменную окружения `KNAAS_EULA_AGREED` непосредственно при запуске Docker-контейнера Kaspersky SD-WAN:

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

Если переменная окружения `KNAAS_EULA_AGREED` не инициализирована или инициализирована со значением `no` (`KNAAS_EULA_AGREED=no`), это означает несогласие с условиями Лицензионного соглашения. В этом случае при запуске Docker-контейнера Kaspersky SD-WAN выдается сообщение об ошибке, и Kaspersky SD-WAN не запускается.

О предоставлении данных

В Kaspersky SD-WAN интегрированы следующие сторонние решения:

- система мониторинга Zabbix;
- платформа для создания облачных сервисов и хранилищ OpenStack;
- географические карты OpenStreetMap.

Персональные данные, которые могут поступать в Zabbix, OpenStack или OpenStreetMap в результате интеграции, не отправляются за периметр инфраструктуры организации.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского".

Интерфейс решения

Управление Kaspersky SD-WAN осуществляется с помощью веб-интерфейса оркестратора. Отображающиеся в меню разделы можно использовать для настройки компонентов решения. Когда вы переходите в раздел, отображается дополнительное меню с подразделами в свернутом виде. Вам нужно навести курсор мыши на значок одного из подразделов, чтобы снова развернуть меню. Вы можете нажать на значок разворачивания », чтобы выключить функцию автоматического сворачивания меню.

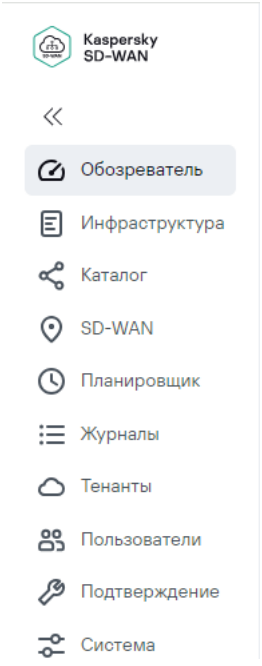
Поддерживается два варианта веб-интерфейса оркестратора:

- *Портал администратора* – предоставляет администраторам полный доступ к управлению компонентами решения.
- *Портал самообслуживания* – предоставляет тенантам доступ к управлению развернутыми для них экземплярами SD-WAN.

Администраторы могут войти на портал самообслуживания тенанта.

Портал администратора

Меню портала администратора изображено на рисунке ниже.

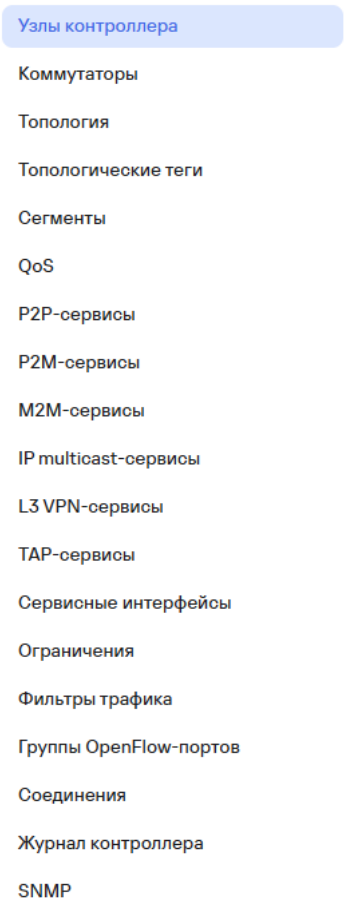


Меню портала администратора

Раздел	Описание
Обозреватель	Информация о текущем состоянии компонентов решения, таких как устройства CPE, а также виртуальные и физические сетевые функции.
Инфраструктура	Инфраструктура организации. В этом разделе вы можете настроить следующие компоненты: • домены; • центры обработки данных; • подсети управления; • контроллеры; • VIM.

Раздел	Описание
Каталог	Шаблоны сетевых сервисов для централизованной настройки сетевых сервисов.
SD-WAN	• **CPE** – устройства CPE для передачи трафика. • **Шаблоны CPE** – шаблоны CPE для централизованной настройки устройств CPE. • **Шаблоны межсетевого экрана** – шаблоны межсетевого экрана для централизованной настройки межсетевого экрана на устройствах CPE. • **Зоны межсетевого экрана** – зоны межсетевого экрана для сетевых интерфейсов и подсетей устройств CPE. • **Шаблоны NetFlow** – шаблоны NetFlow для отслеживания информации о пакетах трафика на устройствах CPE. • **Справочники APN** – список справочников для автоматической конфигурации APN для интерфейсов с типом QMI на устройствах CPE. • **IPAM** – диапазоны IP-адресов и подсетей для устройств CPE. • **Прошивка** – прошивки устройств CPE. • **Сертификаты** – сертификаты устройств CPE. • **Экземпляры SD-WAN** – развернутые экземпляры SD-WAN. • **Шаблоны экземпляров SD-WAN** – шаблоны экземпляра SD-WAN для централизованной настройки и развертывания экземпляров SD-WAN. • **Пулы экземпляров SD-WAN** – пулы экземпляров SD-WAN. • **Шаблоны UNI** – шаблоны UNI для централизованного создания UNI на устройствах CPE.
Планировщик	Задачи, которые будут выполнены позже.
Журналы	Журналы компонентов решения, таких как устройства CPE, а также виртуальные и физические сетевые функции.
Тенанты	Тенанты решения.
Пользователи	Пользователи решения. В этом разделе вы можете настроить следующие компоненты: • пользователей; • права доступа; • группы LDAP-пользователей; • LDAP-подключения.
Подтверждение	Запросы на подтверждение действий пользователей.
Система	• **Мониторинг** – параметры Zabbix-сервера для мониторинга компонентов решения. • **Оповещения** – параметры отправки уведомлений пользователям на электронную почту. • **Журнал оркестратора** – уровень детализации журналов Docker-контейнеров. • **Пользовательские сеансы** – параметры пользовательских сеансов. • **API** – API оркестратора. • **Другое** – дополнительные параметры.

Контроллер имеет отдельное меню настройки (см. рисунок ниже). Более подробно меню настройки контроллера описано в статье Просмотр информации об узлах контроллера.



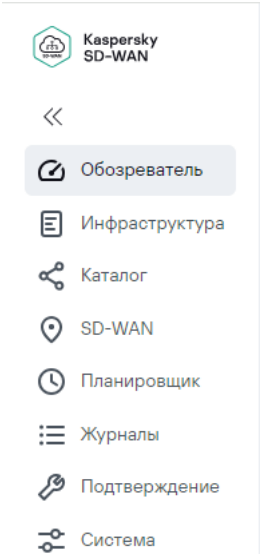
Меню настройки контроллера на портале администратора

Раздел	Описание
Узлы контроллера	Информация о текущем состоянии узлов контроллера.
Коммутаторы	Дополнительные параметры устройств CPE и коммутаторов.
Топология	Графическая топология экземпляра SD-WAN.
Топологические теги	Топологические теги для построения соединений между устройствами CPE.
Сегменты	Сегменты, образованные из устройств CPE и коммутаторов.
QoS	Параметры качества обслуживания. В этом разделе вы можете настроить следующие компоненты: • классы трафика; • классификаторы трафика; • правила качества обслуживания.
P2P-сервисы	Транспортные сервисы Point-to-Point.
P2M-сервисы	Транспортные сервисы Point-to-Multipoint.
M2M-сервисы	Транспортные сервисы Multipoint-to-Multipoint.
IP multicast-сервисы	Транспортные сервисы IP multicast.
L3 VPN-сервисы	Транспортные сервисы L3 VPN.
TAP-сервисы	TAP-сервисы (Test Access Point) для зеркалирования трафика.
Сервисные интерфейсы	Сервисные интерфейсы устройств CPE и коммутаторов.
Ограничения	Ограничения Manual-TE и пороговые ограничения для обеспечения качества обслуживания.

Раздел	Описание
Фильтры трафика	Фильтры трафика для обеспечения качества обслуживания.
Группы OpenFlow-портов	Группы OpenFlow-портов.
Соединения	Соединения между устройствами CPE и коммутаторами, а также соединения между устройствами CPE.
Журналы	Уровень детализации журналов Docker-контейнеров.
SNMP	Параметры мониторинга устройств CPE, а также виртуальных сетевых функций и физических сетевых функций с помощью протокола SNMP.

Портал самообслуживания

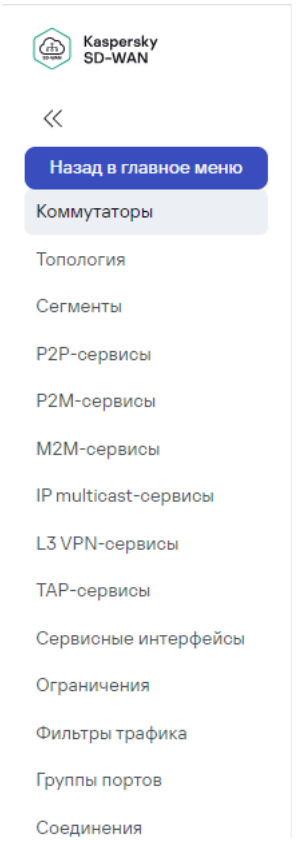
Меню портала самообслуживания изображено на рисунке ниже.



Меню портала самообслуживания

Раздел	Описание
Обозреватель	Информация о текущем состоянии компонентов решения, таких как устройства CPE и сетевые функции.
Инфраструктура	Инфраструктура организации. В этом разделе вы можете настроить контроллеры.
Каталог	Сетевые сервисы для передачи трафика и виртуализации сетевых функций.
SD-WAN	• **CPE** – устройства CPE для передачи трафика. • **Шаблоны CPE** – шаблоны CPE для централизованной настройки устройств CPE. • **Шаблоны межсетевого экрана** – шаблоны межсетевого экрана для централизованной настройки межсетевого экрана на устройствах CPE. • **Зоны межсетевого экрана** – зоны межсетевого экрана для сетевых интерфейсов и подсетей устройств CPE. • **Шаблоны NetFlow** – шаблоны NetFlow для отслеживания информации о пакетах трафика на устройствах CPE. • **IPAM** – диапазоны IP-адресов и подсетей для устройств CPE. • **Шаблоны UNI** – шаблоны UNI для централизованного создания UNI на устройствах CPE.
Планировщик	Задачи, которые будут выполнены позже.
Журналы	Журналы компонентов решения, таких как устройства CPE, а также виртуальные и физические сетевые функции.
Подтверждение	Запросы на подтверждение действий пользователей.
Система	• **Оповещения** – параметры отправки уведомлений пользователям на электронную почту. • **Пользовательские сеансы** – параметры пользовательских сеансов.

Контроллер имеет отдельное меню настройки (см. рисунок ниже).



Раздел	Описание
Коммутаторы	Дополнительные параметры устройств CPE и коммутаторов.
Топология	Графическая топология экземпляра SD-WAN.
Сегменты	Сегменты, образованные из устройств CPE и коммутаторов.
P2P-сервисы	Транспортные сервисы Point-to-Point.
P2M-сервисы	Транспортные сервисы Point-to-Multipoint.
M2M-сервисы	Транспортные сервисы Multipoint-to-Multipoint.
IP multicast-сервисы	Транспортные сервисы IP multicast.
L3 VPN-сервисы	Транспортные сервисы L3 VPN.
TAP-сервисы	TAP-сервисы для зеркалирования трафика.
Сервисные интерфейсы	Сервисные интерфейсы устройств CPE и коммутаторов.
Ограничения	Ограничения Manual-TE и пороговые ограничения для обеспечения качества обслуживания.
Фильтры трафика	Фильтры трафика для обеспечения качества обслуживания.
Группы OpenFlow-портов	Группы OpenFlow-портов.
Соединения	Соединения между устройствами CPE и коммутаторами, а также соединения между устройствами CPE.

Установка и сброс страницы по умолчанию

Страница по умолчанию – это раздел или подраздел меню, который автоматически отображается после того, как вы входите в веб-интерфейс оркестратора.

Чтобы установить или сбросить страницу по умолчанию:

1. Перейдите в раздел или подраздел веб-интерфейса оркестратора, который вы хотите установить как страницу по умолчанию.
2. Откройте меню настройки веб-интерфейса в верхней правой части страницы.
3. В меню выберите **Страница по умолчанию** → **Сделать страницей по умолчанию**.

   В верхней части страницы отобразится сообщение *Страница по умолчанию установлена*.
4. Если вы хотите сбросить страницу по умолчанию, выберите **Страница по умолчанию** → **Сбросить страницу по умолчанию**.

   В верхней части страницы отобразится сообщение *Страница по умолчанию сброшена*. Страницей по умолчанию станет раздел **Обозреватель**.

Переключение между светлым и темным режимом веб-интерфейса оркестратора

Чтобы переключиться между светлым и темным режимом веб-интерфейса оркестратора:

1. Откройте меню настройки веб-интерфейса в верхней правой части страницы.
2. В меню включите или выключите переключатель **Темный режим**.

Изменение языка веб-интерфейса оркестратора

Веб-интерфейс оркестратора поддерживает следующие языки:

- Английский
- Русский
- Испанский (Мексика)
- Португальский (Бразилия)

Чтобы изменить язык веб-интерфейса оркестратора:

1. Откройте меню настройки веб-интерфейса в верхней правой части страницы.
2. В меню выберите пункт с символом глобуса ⊕ и названием текущего языка интерфейса и в раскрывающемся списке выберите нужный язык.

Работа с таблицами компонентов решения

Компоненты решения, такие как пользователи, сетевые интерфейсы и BGP-соседи, отображаются в таблицах. Для работы с таблицами используются следующие элементы:

- Значок настройки, с помощью которого вы можете выполнять следующие действия:
  - Обновить таблицу, нажав на значок настройки → **Перезагрузить**. Вы также можете обновить таблицу с помощью значка обновления.
  - Сбросить ширину столбцов таблицы до ширины по умолчанию, нажав на значок настройки → **Сбросить ширину столбцов**.
  - Выбрать, какие столбцы отображаются в таблице. Для этого вам нужно нажать на значок настройки и установить флажки рядом со столбцами, которые вы хотите отобразить.
- Значок поиска, на который вы можете нажать и ввести критерии поиска. После введения критериев поиска в таблице отображаются соответствующие записи.
- Фильтры статуса для просмотра записей с выбранным статусом.
- Фильтры времени для просмотра записей за выбранный период:
  - **Все время**;
  - **Год**;
  - **Месяц**;
  - **Неделя**;
  - **День**.

  Вы можете указать период вручную с помощью полей в верхней части таблицы.
- Кнопка **Действия** для одновременного выполнения действий с записями, рядом с которыми вы установили флажки. Например, в таблице устройств CPE вы можете одновременно удалить несколько устройств CPE.

Вы можете настроить ширину каждого столбца таблицы с помощью значков в виде трех точек, которые отображаются между именами столбцов.

Переход к API оркестратора

Чтобы перейти к API оркестратора,

1. В меню перейдите в раздел **Система**.

   По умолчанию выбрана вкладка **Мониторинг**, на которой отображаются параметры подключения к серверу Zabbix.

2. Выберите вкладку **API**.

Откроется список API-команд, доступных для управления оркестратором.

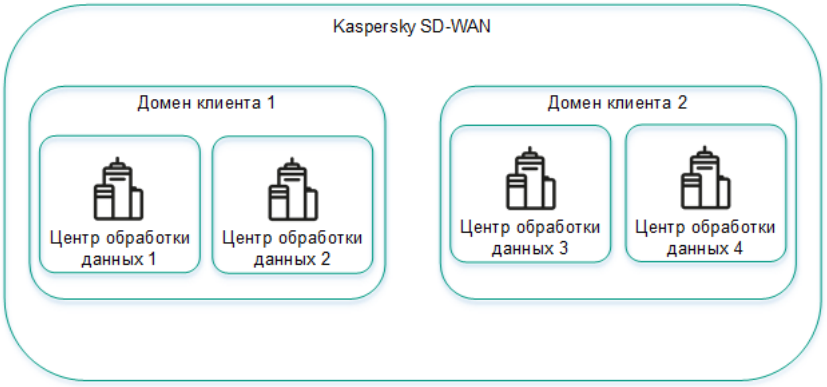
Управление инфраструктурой Kaspersky SD-WAN

Площадки, на которых вы развертываете все компоненты Kaspersky SD-WAN, кроме устройств CPE, называются *центрами обработки данных* (далее также ЦОД). Вам нужно добавить центры обработки данных в веб-интерфейс оркестратора, чтобы управлять контроллерами и VIM, а также указать сервер Zabbix-прокси для настройки мониторинга компонентов решения.

При наличии большого количества центров обработки данных их можно добавить в домены. *Доменами* называются логические группы, которые объединяют центры обработки данных по определенному признаку, например по географическому расположению. Перед добавлением центров обработки данных вам нужно создать хотя бы один домен. Вы можете перемещать центры обработки данных между доменами.

В каждом центре обработки данных необходимо создать хотя бы одну подсеть управления, чтобы назначать устройствам CPE и виртуальным сетевым функциям IP-адреса, DNS-серверы и статические маршруты.

На рисунке ниже изображена схема организации. Компоненты Kaspersky SD-WAN развернуты в четырех центрах обработки данных. Организация предоставляет решение двум клиентам, для каждого из которых развернут экземпляр SD-WAN. Для развертывания каждого экземпляра SD-WAN используется по два центра обработки данных. Центры обработки данных добавлены в соответствующие клиентам домены.



Пример организации с доменами и центрами обработки данных

Работа с доменами

Вы можете просмотреть список доменов в разделе **Инфраструктура** в панели **Ресурсы**. Под доменами в списке отображаются добавленные в них центры обработки данных.

Создание домена

Чтобы создать домен:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В верхней части страницы нажмите на кнопку **+ Домен**.

3. В открывшемся окне в поле **Имя** введите имя домена. Максимальная длина имени: 50 символов.

4. При необходимости в поле **Описание** введите краткое описание домена. Максимальная длина описания: 100 символов.

5. Нажмите на кнопку **Создать**.

Домен будет создан и отобразится в панели **Ресурсы**.

Вы можете добавить в домен центры обработки данных при добавлении центров обработки данных.

Изменение домена

Чтобы изменить домен:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** нажмите на значок настройки → **Изменить** рядом с доменом, который вы хотите изменить.

3. В открывшемся окне при необходимости измените имя и/или краткое описание домена.

4. Нажмите на кнопку **Сохранить**.

Домен будет изменен и обновится в панели **Ресурсы**.

Удаление домена

Перед удалением домена вам нужно удалить центры обработки данных, добавленные в домен.

Удаленные домены невозможно восстановить.

Чтобы удалить домен:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** нажмите на значок настройки → **Удалить** рядом с доменом, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Домен будет удален и перестанет отображаться в панели **Ресурсы**.

Работа с центрами обработки данных

Списки центров обработки данных отображаются в разделе **Инфраструктура** в панели **Ресурсы** под доменами. Перед добавлением центров обработки данных вам нужно создать хотя бы один домен.

Добавление центра обработки данных

Чтобы добавить центр обработки данных:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В верхней части страницы нажмите на кнопку **+ Центр обработки данных**.

3. В открывшемся окне в поле **Имя** введите имя центра обработки данных. Максимальная длина имени: 50 символов.

4. При необходимости в поле **Описание** введите краткое описание центра обработки данных. Максимальная длина описания: 100 символов.

5. В раскрывающемся списке **Домен** выберите созданный домен, в который вы хотите добавить центр обработки данных. После добавления центр обработки данных можно переместить в другой домен.

6. Если вы хотите развертывать виртуальные сетевые функции и запускать скрипты на устройствах CPE, в поле **VNFM URL** введите веб-адрес менеджера виртуальных сетевых функций, к которому подключается оркестратор. Вы можете убедиться в доступности VNFM, нажав на кнопку **Проверить соединение**.

7. При необходимости в поле **Расположение** введите адрес центра обработки данных.

8. Нажмите на кнопку **Создать**.

Центр обработки данных будет добавлен и отобразится в панели **Ресурсы**.

Изменение центра обработки данных

Чтобы изменить центр обработки данных:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** нажмите на значок настройки → **Изменить** рядом с центром обработки данных, который вы хотите изменить.

3. В открывшемся окне при необходимости измените следующие параметры:

   - имя центра обработки данных;
   - краткое описание центра обработки данных;
   - веб-адрес менеджера виртуальных сетевых функций;
   - адрес центра обработки данных.

4. Нажмите на кнопку **Сохранить**.

Центр обработки данных будет изменен и обновится в панели **Ресурсы**.

Перемещение центра обработки данных в другой домен

Чтобы переместить центр обработки данных в другой домен:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** нажмите на значок настройки → **Мигрировать** рядом с центром обработки данных, который вы хотите переместить в другой домен.

3. В открывшемся окне выберите созданный домен, в который вы хотите переместить центр обработки данных.

4. Нажмите на кнопку **Мигрировать**.

Центр обработки данных будет перемещен в новый домен и отобразится под новым доменом в панели **Ресурсы**.

Удаление центра обработки данных

Когда вы удаляете центр обработки данных, вы теряете возможность управлять контроллерами, VIM и подсетями управления в рамках центра обработки данных. Вы также теряете возможность указать сервер Zabbix-прокси для настройки мониторинга компонентов решения.

Удаленные центры обработки данных невозможно восстановить.

Чтобы удалить центр обработки данных:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** нажмите на значок настройки → **Удалить** рядом с центром обработки данных, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Центр обработки данных будет удален и перестанет отображаться в панели **Ресурсы**.

Работа с подсетями управления

Для просмотра таблицы подсетей управления вам нужно в меню перейти в раздел **Инфраструктура**, нажать на добавленный центр обработки данных и выбрать вкладку **IPAM**. Информация о подсетях управления отображается в следующих столбцах таблицы:

- **Имя** – имя подсети управления.
- **Тип** – тип подсети. Временно поддерживаются только подсети управления.
- **CIDR** – IPv4-префикс подсети управления.
- **Шлюз** – IP-адреса шлюзов, которые подсеть управления назначает виртуальным сетевым функциям.
- **Диапазон IP** – диапазоны IP-адресов, из которых подсеть управления назначает IP-адреса устройствам CPE и виртуальным сетевым функциям.
- **DNS** – IPv4-адреса DNS-серверов, которые подсеть управления назначает виртуальным сетевым функциям.
- **Статические маршруты** – IPv4-адреса источника и назначения статических маршрутов, которые подсеть управления назначает виртуальным сетевым функциям.
- **Использование** – количество IP-адресов, которые подсеть управления назначила устройствам CPE и виртуальным сетевым функциям.

Вы можете посмотреть таблицу устройств CPE и виртуальных сетевых функций, которым подсеть управления назначила IP-адреса. Для этого выберите вкладку **Использование**. Информация об устройствах CPE и виртуальных сетевых функциях отображается в следующих столбцах таблицы:

- **Имя** – имя подсети управления, которая назначила устройству CPE или виртуальной сетевой функции IP-адрес.
- **IP** – IP-адрес, назначенный устройству CPE или виртуальной сетевой функции.
- **Имя клиента** – имя устройства CPE или виртуальной сетевой функции.
- **Тип клиента** – информация о том, назначила ли подсеть управления IP-адрес устройству CPE или виртуальной сетевой функции:
  - **VNF**.
  - **CPE**.
- **Тенант** – тенант, которому добавлено устройство CPE или назначена виртуальная сетевая функция.

Действия, которые вы можете выполнить с таблицами, описаны в инструкции Работа с таблицами компонентов решения.

Создание подсети управления

Чтобы создать подсеть управления:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** выберите созданный домен, после чего выберите добавленный центр обработки данных, в котором вы хотите создать подсеть управления. После создания подсеть управления невозможно переместить в другой центр обработки данных.

3. Выберите вкладку **IPAM**.

   По умолчанию выбрана вкладка **Подсеть**, на которой отображается таблица подсетей управления.

4. В верхней части страницы нажмите на кнопку **+ Подсеть**.

5. В поле **Имя** введите имя подсети управления.

6. В раскрывающемся списке **Версия IP** выберите версию IP-адресов в подсети управления:
   - **IPv4**. Это значение выбрано по умолчанию.
   - **IPv6**.

7. В поле **CIDR** введите IPv4-префикс подсети управления.

8. Если вы хотите, чтобы подсеть управления назначала виртуальным сетевым функциям указанный шлюз, в поле **Шлюз** введите IPv4-адрес шлюза.

9. Укажите диапазон IP-адресов, из которого подсеть управления назначает IP-адреса устройствам CPE и виртуальным сетевым функциям. Для этого в блоке **Диапазон IP** нажмите на кнопку **+ Добавить** и в отобразившихся полях введите начальное и конечное значения диапазона IP-адресов.

   Диапазон IP-адресов будет указан и отобразится в блоке **Диапазон IP**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазоны IP-адресов. Для удаления диапазона IP-адресов нажмите рядом с ним на значок удаления ✕.

10. Укажите DNS-сервер, который подсеть управления назначает виртуальным сетевым функциям. Для этого в блоке **DNS** нажмите на кнопку **+ Добавить** и в отобразившемся поле введите IPv4-адрес DNS-сервера.

    DNS-сервер будет указан и отобразится в блоке **DNS**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на значок удаления ✕.

11. Укажите статический маршрут, который подсеть управления назначает виртуальным сетевым функциям. Для этого в блоке **Статические маршруты** нажмите на кнопку **+ Добавить** и в отобразившихся полях введите IPv4-адреса источника и назначения статического маршрута.

    Статический маршрут будет указан и отобразится в блоке **Статические маршруты**. Вы можете указать несколько статических маршрутов и удалить статические маршруты. Для удаления статического маршрута нажмите рядом с ним на значок удаления ✕.

12. Нажмите на кнопку **Создать**.

Подсеть управления будет создана и отобразится в таблице.

Изменение подсети управления

Чтобы изменить подсеть управления:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** выберите созданный домен, после чего выберите добавленный центр обработки данных, в котором вы создали подсеть управления.

3. Выберите вкладку **IPAM**.

   По умолчанию выбрана вкладка **Подсеть**, на которой отображается таблица подсетей управления.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с подсетью управления, которую вы хотите изменить.

5. В открывшемся окне при необходимости измените следующие параметры:

   - имя подсети управления;
   - IPv4-префикс подсети управления;
   - IPv4-адреса шлюзов, которые подсеть управления назначает виртуальным сетевым функциям;
   - диапазоны IP-адресов, из которых подсеть управления назначает IP-адреса устройствам CPE и виртуальным сетевым функциям;
   - DNS-серверы, которые подсеть управления назначает виртуальным сетевым функциям;
   - статические маршруты, которые подсеть управления назначает виртуальным сетевым функциям.

6. Нажмите на кнопку **Сохранить**.

Подсеть управления будет изменена и обновится в таблице.

Удаление подсети управления

Удаленные подсети управления невозможно восстановить.

Чтобы удалить подсеть управления:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** выберите созданный домен, после чего выберите добавленный центр обработки данных, в котором вы создали подсеть управления.

3. Выберите вкладку **IPAM**.

   По умолчанию выбрана вкладка **Подсеть**, на которой отображается таблица подсетей управления.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с подсетью управления, которую вы хотите удалить.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Подсеть управления будет удалена и перестанет отображаться в таблице.

Работа с контроллерами

Для просмотра таблицы контроллеров вам нужно в меню перейти в раздел **Инфраструктура**, нажать на созданный центр обработки данных и выбрать вкладку **Сетевые ресурсы**. Информация о контроллерах отображается в следующих столбцах таблицы:

- **Имя** – имя контроллера.
- **Транспортная/сервисная стратегия** – используемая транспортная стратегия.
- **Тип подключения** – тип подключения устройств CPE к контроллеру:
  - **Unicast**.
  - **Multicast**.
- **Статус кластера** – статус кластера узлов контроллера:
  - **Работает** – кластер работает в штатном режиме.
  - **Ошибка** – при работе кластера возникла ошибка.
  - **Не работает** – кластер не работает.
- **Узлы контроллера** – IP-адреса узлов контроллера.
- **Статус узлов** – статус узлов контроллера:
  - **Подключен** – узел подключен к контроллеру.
  - **Отключен** – узел не подключен к контроллеру.
  - **Недоступен** – узел недоступен.
  - **Неизвестно** – статус узла неизвестен.

- **Роль в кластере** – роль узла в кластере:
  - **Основной** – узел подключен к контроллеру и является основным в кластере.
  - **Второстепенный** – узел подключен к контроллеру и является второстепенным в кластере.
  - **Единственный** – узел подключен к контроллеру и является единственным в кластере.
  - **Арбитр** – узел является арбитром.
  - **Подключен (смена роли)** – происходит смена роли узла в кластере.
  - **Не в кластере** – узел не добавлен в кластер.
  - **Недоступен** – узел недоступен.
  - **Неизвестно** – статус узла неизвестен.
- **Активный узел для операций чтения gRPC** – выбран ли узел в качестве приоритетного для операций чтения при балансировке нагрузки.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Изменение контроллера

Чтобы изменить контроллер:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Изменить** рядом с контроллером, который вы хотите изменить.

3. В открывшемся окне в поле **Имя** введите имя контроллера. Диапазон значений: от 1 до 128 символов.

4. При необходимости в поле **Описание** введите краткое описание контроллера.

5. В поле **Установить контроллер на <1>/<3>/<5> серверах** выберите количество узлов контроллера.

6. В раскрывающемся списке **Тип подключения** выберите тип подключения устройств CPE к контроллеру:
   - **Unicast**.
   - **Multicast**.

7. Настройте узел контроллера:

   a. В поле **IP-адрес или имя хоста** введите IP-адрес или имя хоста узла контроллера.

   b. В поле **gRPC-порт** введите номер gRPC-порта узла контроллера.

   c. В поле **JGroups-порт** введите номер JGroups-порта узла контроллера.

   d. Если вы хотите сделать узел контроллера основным, выберите вариант **Основной**.

   Вы можете настроить несколько узлов контроллера.

8. Если требуется изменить распределение нагрузки при чтении данных между узлами в кластере контроллера, выберите в раскрывающемся списке **Режим балансировки операций чтения gRPC** нужный режим балансировки:

   - **Только основной узел**.

     Операции чтения выполняются только через основной узел кластера.

   - **Приоритет случайно выбранному второстепенному узлу**.

     Операции чтения выполняются с приоритетом через случайно выбранный второстепенный узел кластера.

   - **Выбрать вручную**.

     Операции чтения выполняются через явно указанный приоритетный узел кластера.

   Если вы выбрали режим **Выбрать вручную**, в появившемся списке **Выбранный узел** выберите приоритетный узел, через который должны выполнятся операции чтения.

9. Нажмите на кнопку **Сохранить**.

Контроллер будет изменен и обновится в таблице.

Перезагрузка контроллера

При перезагрузке контроллера его свойства сбрасываются до значений по умолчанию. Это может помочь устранить ошибки.

Чтобы перезагрузить контроллер:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Перезагрузить** рядом с контроллером, который вы хотите перезагрузить.

3. В открывшемся окне подтверждения нажмите на кнопку **Перезагрузить**.

Контроллер будет перезагружен.

Восстановление параметров контроллера

Вы можете скачать файл с параметрами контроллера, которые вы указали в меню настройки контроллера. Например, файл содержит параметры транспортных сервисов и качества обслуживания. При необходимости параметры контроллера можно восстановить с помощью скачанного файла.

Чтобы восстановить параметры контроллера:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Скачать резервный файл** рядом с контроллером, файл с параметрами которого вы хотите скачать.

   На ваше локальное устройство сохранится файл с параметрами контроллера в формате YAML.

3. Нажмите на кнопку **Управление** → **Восстановить** рядом с контроллером, параметры которого вы хотите восстановить.

4. В открывшемся окне укажите путь к скачанному файлу с параметрами контроллера.

5. Нажмите на кнопку **Восстановить**.

Контроллер будет восстановлен с параметрами, соответствующими файлу с параметрами контроллера.

Включение и выключение режима обслуживания на контроллере

Вы можете включить режим обслуживания на контроллере при проведении работ, связанных с сетью SD-WAN, чтобы минимизировать влияние контроллера на участки сети SD-WAN, на которых не ведутся работы. В режиме обслуживания контроллер следит за состоянием сети SD-WAN, но не выполняет никаких действий при изменении параметров сети SD-WAN. Например, в режиме обслуживания контроллер не перестраивает соединения и пути, не переписывает MAC-адреса сервисных интерфейсов и не изменяет транспортные сервисы.

Когда вы выключаете режим обслуживания, контроллер выполняет действия, связанные с изменениями, которые вы внесли в параметры сети SD-WAN.

Чтобы включить или выключить режим обслуживания на контроллере:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Выполните одно из следующих действий:

   - Если вы хотите включить режим обслуживания на контроллере, нажмите рядом с ним на кнопку **Управление** → **Включить режим ТО**.

   - Если вы хотите выключить режим обслуживания на контроллере, нажмите рядом с ним на кнопку **Управление** → **Выключить режим ТО**.

Режим обслуживания будет включен или выключен на контроллере.

Удаление контроллера

Удаленные контроллеры невозможно восстановить.

Чтобы удалить контроллер:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Удалить** рядом с контроллером, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Контроллер будет удален и перестанет отображаться в таблице.

Работа со свойствами контроллера

Свойства регулируют работу контроллера. Каждое свойство имеет *метод изменения*, определяющий, можно ли изменить значение свойства, и в какой момент изменение вступает в силу. Существуют следующие методы изменения:

- **Read-only** – свойство невозможно изменить.
- **Reload** – при изменении свойства оркестратор отправляет новое значение в базу данных контроллера. Новое значение вступает в силу после перезагрузки контроллера.

  Значение свойства, которое находится в базе данных, но еще не вступило в силу, называется *планируемым значением*. Вы можете удалить планируемое значение до перезагрузки контроллера, чтобы сохранить текущее значение.
- **Runtime** – при изменении свойства новое значение сразу вступает в силу.

Изменение свойств может привести к нестабильной работе контроллера, поэтому мы рекомендуем обратиться в техническую поддержку "Лаборатории Касперского" перед началом работы со свойствами.

Вы можете посмотреть таблицу всех или только изменяемых свойств контроллера:

- Для просмотра таблицы всех свойств контроллера вам нужно в меню перейти в раздел **Инфраструктура**, нажать на добавленный центр обработки данных, выбрать вкладку **Сетевые ресурсы** и нажать на кнопку **Управление** → **Свойства** рядом с контроллером.
- Для просмотра таблицы изменяемых свойств контроллера вам нужно в меню перейти в раздел **Инфраструктура**, нажать на добавленный центр обработки данных, выбрать вкладку **Сетевые ресурсы**, нажать на кнопку **Управление** → **Свойства** рядом с контроллером и выбрать вкладку **Изменяемые свойства**.

Информация о свойствах контроллера отображается в следующих столбцах таблицы:

- **Метод изменения** – метод изменения свойства.
- **Свойство** – имя свойства.
- **Текущее значение** – текущее значение свойства.
- **Планируемое значение** – планируемое значение свойства. Этот столбец отображается только на вкладке **Изменяемые свойства**.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Описание изменяемых свойств контроллера

Изменение свойств может привести к нестабильной работе контроллера, поэтому мы рекомендуем обратиться в техническую поддержку "Лаборатории Касперского" перед началом работы со свойствами.

Свойство	Описание
`controller.buffers.in`	Размер в байтах буфера входящих от коммутаторов сообщений на контроллере.
`controller.buffers.out`	Размер в байтах буфера исходящих коммутаторам сообщений на контроллере.
`controller.listen.port`	Номер начального порта в диапазоне портов коммутаторов. В диапазон добавляются порты с тремя следующими по порядку номерами. Например, если вы вводите `6553`, в диапазон портов коммутаторов входят порты с номерами 6553, 6554, 6555, 6556.
`controller.sockets.config.nodelay`	Использование параметра `TCP_NODELAY` для управляющих сессий между коммутаторами и контроллером. Возможные значения: • `true`; • `false`.
`controller.sockets.mode.epoll`	Использование контроллером системы epoll при работе с коммутаторами. Возможные значения: • `true`; • `false`.
`controller.sockets.timeouts.idle.both`	Время в миллисекундах, при истечении которого управляющие сессии между коммутаторами и контроллером переходят в состояние ожидания при отсутствии операций чтения и записи. Отсчет времени начинается заново при каждом выполнении операции чтения или записи.
`controller.sockets.timeouts.idle.read`	Время в миллисекундах, при истечении которого управляющие сессии между коммутаторами и контроллером переходят в состояние ожидания при отсутствии операций чтения. Отсчет времени начинается заново при каждом выполнении операции чтения.
`controller.sockets.timeouts.idle.write`	Время в миллисекундах, при истечении которого управляющие сессии между коммутаторами и контроллером переходят в состояние ожидания при отсутствии операций записи. Отсчет времени начинается заново при каждом выполнении операции записи.
`controller.threads.affinity`	Потоки Netty предпочтительно запускаются на разных ядрах центральных процессоров для разных коммутаторов. Возможные значения: • `true`; • `false`.
`controller.threads.boss`	Количество потоков Netty для обработки новых подключений коммутаторов.
`controller.tls.ca.certificate.path`	Путь к файлу в формате PEM корневого сертификата, которым подписан OpenFlow-сертификат.
`controller.tls.certificate.path`	Путь к файлу в формате PEM сертификата шифрования OpenFlow-трафика между контроллером и коммутаторами.
`controller.tls.private.key.path`	Путь к файлу в формате PEM с приватным ключом OpenFlow-сертификата.
`controller.watermark.high`	Количество байт в буфере Netty управляющей сессии между коммутаторами и контроллером, при котором запись в сессию осуществляется через очередь.
`controller.watermark.low`	Количество байт в буфере Netty управляющей сессии между коммутаторами и контроллером, при котором запись в сессию снова осуществляется без очереди. Это свойство используется, когда количество байт достигает значения свойства `controller.watermark.high`.
`core.catcher.meter.value.kbits`	Пропускная способность полисера на коммутаторах при отправке пакетов трафика через управляющую сессию между коммутаторами и контроллером. Пакеты трафика копируются flow-правилами для перехвата.
`core.drop.rule.idle.sec`	Время в секундах, при истечении которого на коммутаторах удаляются flow-правила, автоматически созданные контроллером при обработке первого перехваченного пакета трафика для блокировки последующих пакетов. Отсчет времени начинается заново при каждом применении flow-правила.

Свойство	Описание
`core.link.bonding.enable`	Объединение (англ. bonding) параллельных соединений между двумя коммутаторами. Возможные значения: • `true`; • `false`.
`core.link.bonding.equal.cost`	Использование алгоритма equal cost при объединении соединений. Возможные значения: • `true`; • `false`. Если вы указываете значение `false`, используется алгоритм unequal cost.
`core.link.bonding.max.links`	Максимальное количество соединений в объединенном соединении.
`core.link.bonding.mode`	Тип группы объединенных соединений. Возможные значения: • `BALANCING` – трафик распределяется по соединениям в соответствии со значением хеша. Хеш подсчитывается на основании полей `IP Proto`, `IP src-dst` и `Port src-dst` пакетов трафика. • `BROADCAST` – трафик дублируется через все соединения.
`core.link.check.ports.status`	Периодическая отправка контроллером LLDP-пакетов только на включенные порты для обнаружения соединений между коммутаторами. Возможные значения: • `true`; • `false`.
`core.link.enabled.ports.only`	Пересылка коммутаторами LLDP-пакетов контроллеру только со включенных портов, когда контроллер пытается обнаружить соединения между коммутаторами. Возможные значения: • `true`; • `false`.
`core.link.liveness.interval`	Интервал времени в миллисекундах для отправки контроллером LLDP-пакетов через соединения коммутаторов.
`core.link.liveness.timeout`	Интервал времени в миллисекундах для получения приемной стороной соединений коммутаторов LLDP-пакетов и пересылки LLDP-пакетов контроллеру. Если в течение указанного времени через соединение не поступает LLDP-пакетов, контроллер считает соединение недоступным.
`core.lldp.sendrem.enabled`	Отправка коммутаторами уведомлений контроллеру при удалении flow-правил, которые отправляют пакеты трафика на контроллер. Возможные значения: • `true`; • `false`.
`core.switch.liveness.interval`	Интервал времени в миллисекундах для проверки подключения коммутаторов к контроллеру.
`core.switch.liveness.timeout`	Время в миллисекундах, в течение которого отключенные коммутаторы повторно подключаются к контроллеру.
`core.tunnel.port.end`	Номер конечного виртуального сетевого интерфейса (англ. virtual network interface, VNI) в диапазоне интерфейсов коммутаторов.
`core.tunnel.port.start`	Номер начального виртуального сетевого интерфейса в диапазоне интерфейсов коммутаторов.
`dampening.link.enabled`	Использование функции Dampening на соединениях. Возможные значения: • `true`; • `false`.
`dampening.link.maxSuppressTime.ms`	Максимальное время в миллисекундах, в течение которого доступ к соединению может быть ограничен. По истечении указанного времени счетчики функции Dampening сбрасываются.

Свойство	Описание
`dampening.link.penalty`	Число, которое прибавляется к показателю Penalty при изменении состояния соединения.
`dampening.link.suppressLevel`	Значение показателя Penalty, при котором доступ к соединению ограничивается.
`dampening.link.updateInterval.ms`	Время в миллисекундах, в течение которого показатель Penalty должен набрать значение свойства `dampening.link.suppressLevel`, чтобы доступ к соединению был ограничен.
`eth.s.type`	Значение IEEE 802.1Q TPID, которое устанавливается как внутренняя метка для пакетов трафика с классификацией трафика Q-in-Q.
`eth.t.type`	Значение IEEE 802.1Q TPID, которое устанавливается как внешняя метка для пакетов трафика с классификацией трафика Q-in-Q.
`inband.statistics.enabled`	Получение статистики на коммутаторах. Статистика содержит информацию сетевых устройствах, к которым подключен коммутатор, а также об используемых портах. Возможные значения: • `true`; • `false`.
`inband.swos.cookie`	Значение поля `cookie` в сообщении запроса статистики с коммутаторов. Возможные значения: • `true`; • `false`. Значение для этого свойства необходимо указать, если для свойства `inband.statistics.enabled` вы указали значение `true`.
`network.control.queue.id`	Идентификатор очереди LLDP-пакетов на коммутаторах.
`notification.all.queue.max.size`	Максимальный размер очереди push-уведомлений на коммутаторах. При превышении размера удаляется первое push-уведомление в очереди.
`openflow.fail2ban.banTimeSec`	Время в секундах, в течение которого IP-адреса и порты коммутаторов блокируются после попытки подключиться к контроллеру с неверным TLS-сертификатом.
`openflow.fail2ban.enabled`	Блокировка IP-адресов и портов коммутаторов после попытки подключиться к контроллеру с неверным TLS-сертификатом. Возможные значения: • `true`; • `false`.
`openflow.fail2ban.findTimeSec`	Время в секундах, в течение которого коммутаторы совершают указанное с помощью свойства `openflow.fail2ban.maxRetry` количество попыток подключения к контроллеру с неверным TLS-сертификатом, чтобы IP-адреса и порты этих коммутаторов были заблокированы.
`openflow.fail2ban.maxRetry`	Количество попыток подключения коммутаторов к контроллеру с неверным TLS-сертификатом, при котором IP-адреса и порты коммутаторов блокируются.
`openflow.io.cpe.rate.limiter.read.byteps`	Это свойство больше не используется.
`openflow.io.cpe.rate.limiter.write.byteps`	Это свойство больше не используется.
`openflow.io.ovs.meters.enabled`	Отправка flow-правилами пакетов трафика на контроллер. Возможные значения: • `true`; • `false`.
`openflow.io.rate.limiter.switch.type-to-rate`	Это свойство больше не используется.
`openflow.io.switch.latency.monitoring.delay.ms`	Интервал времени в миллисекундах для проверки задержки между контроллером и коммутаторами.

Свойство	Описание
`openflow.io.switch.latency.monitoring.enabled`	Проверка задержки между контроллером и коммутаторами. Возможные значения: • `true`; • `false`.
`openflow.io.switch.latency.sma.initial.drop.size`	Количество начальных пакетов трафика на коммутаторах, которые не используются при подсчете статистики.
`openflow.io.switch.latency.sma.window.size`	Количество последних пакетов трафика на коммутаторах, которые используются при подсчете статистики.
`openflow.io.switch.messages.chunk.bytes`	Размер в байтах блоков (англ. chunk) сериализованных OpenFlow-сообщений, которые контроллер отправляет коммутаторам.
`openflow.io.switch.messages.window.size`	Максимальное количество блоков сериализованных OpenFlow-сообщений в очереди на контроллере.
`openflow.io.switch.rate.limiter.read.byteps`	Это свойство больше не используется.
`openflow.io.switch.rate.limiter.write.byteps`	Это свойство больше не используется.
`openflow.io.vtep.rate.limiter.read.byteps`	Это свойство больше не используется.
`openflow.io.vtep.rate.limiter.write.byteps`	Это свойство больше не используется.
`segment.path.num.max`	Максимальное количество путей в сегменте.
`segment.path.spf.num.max`	Максимальное количество SPF-путей для автоматической балансировки.
`table-miss.mode`	Действие, которое коммутаторы выполняют с пакетами трафика, не попавшими ни в одну из OpenFlow-таблиц. Возможные значения: • `DROP` – отбросить пакеты трафика. • `TO_CTL` – отправить пакеты трафика на контроллер.
`topology.cfm.enabled`	Использование Connectivity Fault Management (CFM) на соединениях. Возможные значения: • `true`; • `false`.
`topology.debug.enabled`	Использование процедур отладки контроллера с помощью протокола gRPC. Возможные значения: • `true`; • `false`.
`topology.intervtep.links.enabled`	Построение соединений между VTEP. Возможные значения: • `true`; • `false`.
`topology.link.charged`	Использование всех соединений в последнюю очередь при маршрутизации трафика независимо от качества связи. Возможные значения: • `true`; • `false`.
`topology.link.discovery.groups.enabled`	Обнаружение соединений по группам. Возможные значения: • `true`; • `false`.
`topology.link.encryption.enabled`	Шифрование трафика на соединениях. Возможные значения: • `true`; • `false`.
`topology.link.encryption.key.update.interval.minutes`	Интервал времени в минутах для обновления ключа дешифровки на соединениях.

Свойство	Описание
`topology.link.error.monitoring.enabled`	Мониторинг ошибок на соединениях. Возможные значения: • `true`; • `false`.
`topology.link.error.threshold.eps`	Пороговое значение количества ошибок в секунду на соединениях.
`topology.link.eu.monitoring.delay.sec`	Интервал времени в секундах для измерения количества ошибок на соединениях и загруженности соединений.
`topology.link.fec.enable`	Использование функции Forward Error Correction (FEC) на соединениях. Возможные значения: • `true`; • `false`.
`topology.link.fec.ratio`	Соотношение между оригинальными пакетами трафика и дополнительными пакетами с избыточным кодом. Вам нужно ввести значение в формате `< количество оригинальных пакетов >: < количество дополнительных пакетов >`.
`topology.link.fec.timeout`	Максимальное время в миллисекундах, в течение которого пакет трафика может находиться в очереди для применения функции FEC.
`topology.link.jitter.monitoring.enabled`	Мониторинг джиттера на соединениях. Возможные значения: • `true`; • `false`.
`topology.link.jitter.threshold.ms`	Пороговое значение времени джиттера в миллисекундах на соединениях.
`topology.link.latency.monitoring.enabled`	Мониторинг задержек на соединениях. Возможные значения: • `true`; • `false`.
`topology.link.latency.threshold.ms`	Пороговое значение времени задержки в миллисекундах на соединениях.
`topology.link.ljp.monitoring.delay.sec`	Интервал времени в секундах для сравнения полученных показателей мониторинга с указанными пороговыми значениями задержек, джиттера и потери пакетов на соединениях.
`topology.link.ljp.stats.collecting.enabled`	Мониторинг задержек, джиттера и потерь пакетов трафика на соединениях. Возможные значения: • `true`; • `false`. Протокол для мониторинга можно указать с помощью свойства `topology.link.ljp.stats.collecting.method`.
`topology.link.ljp.stats.collecting.lldp.window`	Размер в байтах дополнительного буфера в каждом LLDP-пакете для показателей мониторинга задержек, джиттера и потерь пакетов трафика на соединениях. Значение для этого свойства необходимо указать, если для свойства `topology.link.ljp.stats.collecting.method` вы указали значение `GENEVE`.
`topology.link.ljp.stats.collecting.method`	Протокол для мониторинга задержек, джиттера и потерь пакетов трафика на соединениях. Возможные значения: • `LLDP`; • `GENEVE`.
`topology.link.ljp.stats.collecting.multiplicity`	Множитель, который применяется на контроллере к показателям мониторинга задержек, джиттера и потерь пакетов трафика на соединениях. Значение для этого свойства необходимо указать, если для свойства `topology.link.ljp.stats.collecting.method` вы указали значение `GENEVE`.

Свойство	Описание
`topology.link.packet.loss.monitoring.enabled`	Мониторинг потерь пакетов трафика на соединениях. Возможные значения: • `true`; • `false`.
`topology.link.packet.loss.threshold.percents`	Пороговое значение процента потерь пакетов трафика на соединениях.
`topology.link.pmtud.scheduler.interval.sec`	Интервал времени в секундах для автоматического определения показателя MTU на соединениях.
`topology.link.pmtud.wait.time.ms`	Время в миллисекундах для ожидания контроллером пакета PMTUD LLDP. Если при истечении этого времени контроллер не получает пакет PMTUD LLDP, контроллер считает, что пакет такого размера невозможно передать через соединение.
`topology.link.threshold.monitoring.delay.sec`	Интервал времени в секундах для мониторинга пороговых значений на соединениях.
`topology.link.threshold.monitoring.enabled`	Мониторинг пороговых значений на соединениях. Возможные значения: • `true`; • `false`.
`topology.link.threshold.monitoring.unban.periods`	Количество успешных проверок подряд для разблокирования соединений. Проверка проводится раз в секунду.
`topology.link.util.monitoring.enabled`	Мониторинг загруженности (использования полосы) соединений. Возможные значения: • `true`; • `false`.
`topology.link.util.threshold.percents`	Пороговое значение загруженности соединений в процентах от скорости сервисных интерфейсов.
`topology.overlay.lldp.sender.concurrent`	Параллельная отправка контроллером LLDP-пакетов для обнаружения соединений. Возможные значения: • `true`; • `false`.
`topology.overlay.lldp.sender.core.pool.size`	Минимальное количество потоков для параллельной отправки контроллером LLDP-пакетов. Значение для этого свойства необходимо указать, если для свойства `topology.overlay.lldp.sender.concurrent` вы указали значение `true`.
`topology.overlay.lldp.sender.max.pool.size`	Максимальное количество потоков для параллельной отправки контроллером LLDP-пакетов. Значение для этого свойства необходимо указать, если для свойства `topology.overlay.lldp.sender.concurrent` вы указали значение `true`.
`topology.overlay.lldp.sender.max.queue.capacity`	Максимальный размер очереди при параллельной отправке контроллером LLDP-пакетов. Значение для этого свойства необходимо указать, если для свойства `topology.overlay.lldp.sender.concurrent` вы указали значение `true`.
`topology.reserve.si.auto.revert.enabled`	Резервный сервисный интерфейс снова становится резервным, если прежний сервисный интерфейс восстанавливает работу. Возможные значения: • `true`; • `false`.

Свойство	Описание
`topology.throttler.timeout.hard.enabled`	Накопление на контроллере физических операций, таких как подключение коммутатора или порта, и выполнение операций при истечении указанного вами времени. Возможные значения: • `true`; • `false`. Время можно указать с помощью свойств `topology.throttler.timeout.hard.ms` и `topology.throttler.timeout.idle.ms`.
`topology.throttler.timeout.hard.ms`	Время в секундах, при истечении которого выполняются накопившиеся на контроллере физические операции. Значение для этого свойства необходимо указать, если для свойства `topology.throttler.timeout.hard.enabled` вы указали значение `true`.
`topology.throttler.timeout.idle.ms`	Время в секундах, при истечении которого выполняются накопившиеся на контроллере физические операции. Отсчет времени начинается заново при каждом появлении физической операции. Значение для этого свойства можно указать, если для свойства `topology.throttler.timeout.hard.enabled` вы указали значение `true`.
`topology.throttler_future.enable`	Системное свойство. Изменение значения этого свойства может привести к потере работоспособности контроллера.
`topology.throttler_future.timeout.sec`	Системное свойство. Изменение значения этого свойства может привести к потере работоспособности контроллера.

Изменение свойства контроллера

Изменения, которые вы вносите в свойства контроллера с методом изменения Runtime, сразу вступают в силу. Изменения, которые вы вносите в свойства контроллера с методом изменения Reload, вступают в силу после перезагрузки контроллера.

Чтобы изменить свойство контроллера:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Свойства** рядом с контроллером, свойство которого вы хотите изменить.

   Откроется страница управления свойствами контроллера. По умолчанию выбрана вкладка **Все свойства**, на которой отображается таблица всех свойств контроллера.

3. Выберите вкладку **Изменяемые свойства**.

   Отобразится таблица изменяемых свойств контроллера.

4. Нажмите на кнопку **Управление** → **Изменить** рядом со свойством контроллера, которое вы хотите изменить.

5. В открывшемся окне в поле **Планируемое значение** введите новое значение свойства контроллера.

6. Нажмите на кнопку **Сохранить**.

Новое значение свойства с методом изменения Runtime отобразится в столбце **Текущее значение**. Новое значение свойства с методом изменения Reload отобразится в столбце **Планируемое значение**.

Удаление запланированных значений свойств контроллера

Вы можете удалить запланированное значение, чтобы отменить изменение свойства контроллера. Это действие применимо только к свойствам с методом изменения Reload.

Удаленные запланированные значения свойств контроллера невозможно восстановить.

Чтобы удалить запланированные значения свойств контроллера:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Свойства** рядом с контроллером, запланированные значения свойств которого вы хотите удалить.

   Откроется страница управления свойствами контроллера. По умолчанию выбрана вкладка **Все свойства**, на которой отображается таблица всех свойств контроллера.

3. Выберите вкладку **Изменяемые свойства**.

   Отобразится таблица изменяемых свойств контроллера.

4. Перейдите к удалению запланированных значений свойств контроллера одним из следующих способов:

   - Если вы хотите удалить запланированное значение отдельного свойства контроллера, нажмите на кнопку **Управление** → **Удалить запланированное значение** рядом этим свойством.

   - Если вы хотите удалить запланированные значения всех свойств контроллера, в верхней части таблицы нажмите на значок настройки → **Удалить все запланированные значения**.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Запланированные значения свойств контроллера будут удалены.

Сброс свойств контроллера до значений по умолчанию

Чтобы сбросить свойства контроллера до значений по умолчанию:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Свойства** рядом с контроллером, свойства которого вы хотите сбросить до значений по умолчанию.

   Откроется страница управления свойствами контроллера. По умолчанию выбрана вкладка **Все свойства**, на которой отображается таблица всех свойств контроллера.

3. Выберите вкладку **Изменяемые свойства**.

   Отобразится таблица изменяемых свойств контроллера.

4. Перейдите к сбросу свойств контроллера одним из следующих способов:

   - Если вы хотите сбросить отдельное свойство контроллера до значения по умолчанию, нажмите на кнопку **Управление** → **Сбросить свойство** рядом этим свойством.

   - Если вы хотите сбросить все свойства контроллера до значений по умолчанию, в верхней части таблицы нажмите на значок настройки → **Сбросить все свойства**.

5. В открывшемся окне подтверждения нажмите на кнопку **Сбросить**.

Свойства контроллера будут сброшены до значений по умолчанию.

Просмотр информации об узлах контроллера

- Чтобы посмотреть информацию об узлах контроллера:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, информацию об узлах которого вы хотите посмотреть.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера. Информация об узлах контроллера отображается в следующих столбцах таблицы:

   - **Адрес** – IP-адрес узла контроллера.
   - **Статус узлов** – статус узлов контроллера:
     - **Подключен** – узел подключен к контроллеру.
     - **Отключен** – узел не подключен к контроллеру.
     - **Недоступен** – узел недоступен.
     - **Неизвестно** – статус узла неизвестен.
   - **Роль в кластере** – роль узла в кластере:
     - **Основной** – узел подключен к контроллеру и является основным в кластере.
     - **Второстепенный** – узел подключен к контроллеру и является второстепенным в кластере.
     - **Единственный** – узел подключен к контроллеру и является единственным в кластере.
     - **Арбитр** – узел является арбитром.
     - **Подключен (смена роли)** – происходит смена роли узла в кластере.
     - **Не в кластере** – узел не добавлен в кластер.
     - **Недоступен** – узел недоступен.
     - **Неизвестно** – статус узла неизвестен.
   - **Активный узел для операций чтения gRPC** – выбран ли узел в качестве приоритетного для операций чтения при балансировке нагрузки.
   - **gRPC-порт** – номер gRPC-порта узла контроллера.
   - **JGroups-порт** – номер JGroups-порта узла контроллера.
   - **Версия** – версия программного обеспечения узла контроллера.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

3. Если вы хотите посмотреть статистику работы узла контроллера, нажмите на кнопку **Управление** → **Статистика** рядом с этим узлом.

4. Если вы хотите посмотреть свойства узла контроллера, нажмите на кнопку **Управление** → **Свойства узла** рядом с этим узлом.

Работа с VIM

Вы можете развернуть VIM в одном из ваших центров обработки данных или на устройстве uCPE. Развертывание VIM в центре обработки данных, подразумевает централизованное управление жизненным циклом виртуальных сетевых функций. Развертывание VIM на устройстве uCPE позволяет доставлять виртуальные сетевые функции на удаленные центры обработки данных и управлять этими функциями локально.

Для просмотра таблицы VIM вам нужно в меню перейти в раздел **Инфраструктура**, нажать на созданный центр обработки данных и выбрать вкладку **IPAM** → **Вычислительные ресурсы**. Информация о VIM отображается в следующих столбцах таблицы:

- **Имя** – имя VIM.
- **Тип** – тип VIM. В Kaspersky SD-WAN в качестве VIM используется облачная платформа OpenStack.
- **Функция** – центр обработки данных или устройство uCPE, на котором развернут VIM.
- **VIM IP** – IP-адрес VIM.
- **Статус** – статус подключения VIM к облачной платформе OpenStack:
  - **Подключено**.
  - **Отключено**.
- **Кластер SDN** – SDN-кластер, к которому подключен OpenStack.
- **За NAT** – VIM находится за NAT (Network Address Translation):
  - **Да**.
  - **Нет**.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Настройка VIM, развернутого в центре обработки данных

Чтобы настроить VIM, развернутый в центре обработки данных:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** выберите созданный домен, после чего выберите добавленный центр обработки данных, в котором вы развернули VIM.

3. Выберите вкладку **Вычислительные ресурсы**.

   Отобразится таблица VIM.

4. В верхней части страницы нажмите на кнопку **+ VIM**.

5. В открывшемся окне в поле **Имя** введите имя VIM.

6. В поле **IP** введите IP-адрес или доменное имя для подключения оркестратора к VIM.

7. В поле **Порт** введите номер порта для подключения оркестратора к службе идентификации VIM. Значение по умолчанию: `5000`.

8. В раскрывающемся списке **Протокол** выберите протокол для подключения оркестратора к VIM:

   - **http**. Это значение выбрано по умолчанию.
   - **https**.

9. В полях **Имя пользователя** и **Пароль** введите имя пользователя и пароль учетной записи с правами администратора для аутентификации оркестратора в облачной платформе OpenStack. Если аутентификация пройдет успешно, оркестратор получит доступ к управлению виртуальной инфраструктурой, доступной администратору.

10. Укажите дополнительные параметры аутентификации оркестратора в облачной платформе OpenStack:

    a. В поле **Проект администратора** введите имя проекта администратора для аутентификации оркестратора в проекте администратора.

    b. В поле **Домен** введите имя OpenStack-домена для аутентификации оркестратора в OpenStack-домене.

11. В раскрывающемся списке **За NAT** выберите, находится ли VIM за NAT:

    - **Включено** – VIM находится за NAT, и при взаимодействии VIM с экземпляром SD-WAN происходит трансляция сетевых адресов.
    - **Выключено** – VIM не находится за NAT. Это значение выбрано по умолчанию.

12. Укажите коэффициенты переподписки физических ресурсов:

    a. В поле **Переподписка ЦП** введите коэффициент переподписки ядер процессора. Значение по умолчанию: `1`.

    b. В поле **Переподписка ОЗУ** введите коэффициент переподписки оперативной памяти. Значение по умолчанию: `1`.

    c. В поле **Переподписка диска** введите коэффициент переподписки дискового пространства. Значение по умолчанию: `1`.

    Коэффициенты переподписки позволяют предоставлять виртуальным машинам больше виртуальных ресурсов, чем доступно физических. Это возможно потому, что виртуальные машины одновременно не используют все доступные физические ресурсы на максимум. Например, если вы указываете коэффициент переподписки `3` для дискового пространства, количество доступного виртуального дискового пространства может в три раза превышать количество доступного на хосте физического дискового пространства.

    При настройке переподписки вам нужно учитывать, как возможности вашего оборудования соотносятся с требованиями виртуальных машин. Если вы указываете высокое значение переподписки для физических ресурсов и виртуальные машины начинают использовать их на максимум, это может привести к задержкам в работе сети и/или полной недоступности некоторых ее участков.

13. В поле **Параллелизм** введите максимальное количество одновременных операций при взаимодействии оркестратора и VIM. Значение по умолчанию: `1`. Этот параметр позволяет увеличить суммарную скорость выполнения операций, но создает дополнительную нагрузку на виртуальную инфраструктуру.

    Мы рекомендуем не изменять значение по умолчанию, если суммарная скорость выполнения операций не является для вас критически важным параметром.

14. В раскрывающемся списке **Кластер SDN** выберите SDN-кластер, к которому подключен OpenStack. Если OpenStack не подключен к SDN-кластеру, выберите значение **Отсутствует**.

15. В поле **Максимальное количество VLAN** введите максимальное количество VLAN, которое может использовать VIM. Этот параметр позволяет оркестратору отслеживать количество сегментов, доступных для использования. Диапазон значений: от 0 до 4094.

16. Если VIM поддерживает SR-IOV, в поле **Физическая сеть SR-IOV** введите имя физической сети (англ. physnet name). Оркестратор использует имя физической сети SR-IOV для подключения виртуальных машин с типом интерфейса SR-IOV.

17. Если для управления вы используете сеть с типом сегментации VLAN, в поле **Физическая VLAN-сеть** введите VLAN-тег.

18. Если в раскрывающемся списке **Кластер SDN** вы выбрали SDN-кластер, настройте подключение к этому кластеру:

    a. Если вы хотите сопоставить логические сети экземпляра SD-WAN с физической сетью, в поле **Физическая OpenStack-сеть** введите имя физической сети.

    b. В раскрывающемся списке **Группа портов** выберите группу портов, через которую все узлы OpenStack подключены к SDN-кластеру.

    c. В раскрывающемся списке **Управляющая группа** выберите группу портов, через которую управляющие узлы OpenStack подключены к SDN-кластеру.

    d. При необходимости в раскрывающемся списке **Вычислительная группа** выберите группу портов, через которую вычислительные узлы OpenStack подключены к SDN-кластеру.

19. Если в раскрывающемся списке **Кластер SDN** вы выбрали **Отсутствует**, настройте сеть:

    a. Если вы хотите сопоставить плоские сети (англ. flat networks) экземпляра SD-WAN с физической сетью, в поле **Плоская физическая сеть** введите имя физической сети.

    b. Если вы хотите сопоставить VXLAN экземпляра SD-WAN с физической сетью, в поле **Физическая VXLAN-сеть** введите имя физической сети.

    c. В раскрывающемся списке **Сегментация управляющей сети** выберите тип сегментации для изоляции и защиты трафика плоскости управления в структуре сети SD-WAN:

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

    d. В поле **ID управляющего сегмента** введите идентификатор сегмента управляющей сети. Диапазон значений зависит от значения, выбранного в раскрывающемся списке **Сегментация управляющей сети**:

    - Если вы выбрали **VLAN**, диапазон значений: от 0 до 4095.
    - Если вы выбрали **VXLAN**, диапазон значений: от 0 до 16 000 000.

    e. В раскрывающемся списке **Port security** выберите, требуется ли включить функцию Port security:

    - **Включено**.
    - **Выключено**.

    f. В поле **Разрешить CIDR** введите IPv4-префикс разрешенной подсети для сети управления.

20. Нажмите на кнопку **Создать**.

VIM будет создан и отобразится в таблице на вкладке **Вычислительные ресурсы**.

Настройка VIM, развернутого на устройстве uCPE

Для настройки VIM, развернутого на устройстве uCPE, вам нужно указать параметры VIM в шаблоне uCPE. Параметры VIM, указанные в шаблоне uCPE, автоматически распространяются на все использующие шаблон uCPE устройства CPE.

Чтобы настроить VIM, развернутый на устройстве uCPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон uCPE, в котором вы хотите настроить VIM.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **VIM**.

   Отобразятся параметры VIM.

4. В поле **Порт** введите номер порта для подключения оркестратора к сервису идентификации VIM. Значение по умолчанию: `5000`.

5. В раскрывающемся списке **Протокол** выберите протокол для подключения оркестратора к VIM:

   - **http**. Это значение выбрано по умолчанию.
   - **https**.

6. В полях **Имя пользователя** и **Пароль** введите имя пользователя и пароль учетной записи с правами администратора для аутентификации оркестратора в облачной платформе OpenStack. Если аутентификация проходит успешно, оркестратор получает доступ к управлению доступной администратору виртуальной инфраструктурой.

7. Укажите дополнительные параметры аутентификации оркестратора в облачной платформе OpenStack:

   a. В поле **Проект администратора** введите имя проекта администратора для аутентификации оркестратора в проекте администратора.

   b. В поле **Домен** введите имя OpenStack-домена для аутентификации оркестратора в OpenStack-домене.

8. Если для управления вы используете сеть с типом сегментации VLAN, в поле **Физическая VLAN-сеть** введите VLAN-тег.

9. В раскрывающемся списке **За NAT** выберите, находится ли VIM за NAT:

   - **Включено** – VIM находится за NAT, и при его взаимодействии с экземпляром SD-WAN происходит преобразование сетевых адресов.
   - **Выключено** – VIM не находится за NAT. Это значение выбрано по умолчанию.

10. Укажите коэффициенты переподписки физических ресурсов:

    a. В поле **Переподписка ЦП** введите коэффициент переподписки ядер процессора. Значение по умолчанию: `1`.

    b. В поле **Переподписка ОЗУ** введите коэффициент переподписки оперативной памяти. Значение по умолчанию: `1`.

    c. В поле **Переподписка диска** введите коэффициент переподписки дискового пространства. Значение по умолчанию: `1`.

    Коэффициенты переподписки позволяют предоставлять виртуальным машинам больше виртуальных ресурсов, чем доступно физических. Это возможно потому, что виртуальные машины одновременно не используют все доступные физические ресурсы на максимум. Например, если вы указываете коэффициент переподписки `3` для дискового пространства, количество доступного виртуального дискового пространства может в три раза превышать количество доступного на хосте физического дискового пространства.

    При настройке переподписки вам нужно учитывать, как возможности вашего оборудования соотносятся с требованиями виртуальных машин. Если вы указываете высокое значение переподписки для физических ресурсов и виртуальные машины начинают использовать их на максимум, это может привести к задержкам в работе сети и/или полной недоступности некоторых ее участков.

11. В поле **Максимальное количество VLAN** введите максимальное количество VLAN, которое может использовать VIM. Этот параметр позволяет оркестратору отслеживать количество сегментов, доступных для использования. Диапазон значений: от 0 до 4094.

12. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE.

Изменение VIM, развернутого в центре обработки данных

Чтобы изменить VIM, развернутый в центре обработки данных:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** выберите созданный домен, после чего выберите добавленный центр обработки данных, в котором вы развернули VIM.

3. Выберите вкладку **Вычислительные ресурсы**.

   Отобразится таблица VIM.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с VIM, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры VIM. Описание параметров см. в инструкции по настройке VIM, развернутого в центре обработки данных.

6. Нажмите на кнопку **Сохранить**.

VIM будет изменен и обновится в таблице.

Просмотр вычислительных ресурсов, используемых VIM

Вы можете посмотреть, насколько VIM использует следующие вычислительные ресурсы:

- центральный процессор;
- оперативная память;
- дисковое пространство;
- сетевые сегменты.

Чтобы посмотреть вычислительные ресурсы, используемые VIM:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** выберите созданный домен, после чего выберите добавленный центр обработки данных, в котором вы развернули VIM.

3. Выберите вкладку **Вычислительные ресурсы**.

   Отобразится таблица VIM.

4. Нажмите на кнопку **Управление** → **Показать использование** рядом с VIM.

Откроется окно с информацией о вычислительных ресурсах, используемых VIM.

Удаление VIM

Удаленные VIM невозможно восстановить.

Чтобы удалить VIM:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** выберите созданный домен, после чего выберите добавленный центр обработки данных, в котором вы развернули VIM.

3. Выберите вкладку **Вычислительные ресурсы**.

   Отобразится таблица VIM.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с VIM, который вы хотите удалить.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

VIM будет удален и перестанет отображаться в таблице.

Управление пользователями и их правами доступа

Для разграничения доступа к порталу администратора и порталу самообслуживания, а также к разделам, подразделам и функциям в решении реализована модель управления доступом на основе ролей (англ. Role Based Access Control, RBAC). Учетные записи пользователей могут иметь следующие роли:

- Администратор – имеет доступ к порталу администратора и порталу самообслуживания.
- Тенант – имеет доступ только к порталу самообслуживания.

При развертывании решения создается пользователь **Administrator** с ролью администратор и пользователь **User** с ролью тенант.

Вы можете создавать локальных и LDAP-пользователей, а также группы LDAP-пользователей. Решение не поддерживает создание групп локальных пользователей. Учетные данные локальных пользователей хранятся в базе данных оркестратора. Учетные данные LDAP-пользователей и групп LDAP-пользователей хранятся на удаленном сервере. Поддерживается удаленный сервер OpenLDAP с Simple-аутентификацией и Simple SSL-аутентификацией, а также Microsoft Active Directory с Kerberos-аутентификацией и Kerberos SSL-аутентификацией.

Вам нужно создать LDAP-подключение, с помощью которого оркестратор подключается к удаленному серверу, после чего создать LDAP-пользователей и/или группы LDAP-пользователей. Созданные LDAP-пользователи и группы LDAP-пользователей могут входить в веб-интерфейс оркестратора, используя свои учетные данные.

Двухфакторная аутентификация

Для повышения общего уровня безопасности решения можно выполнять двухфакторную аутентификацию (англ. two-factor authentication) пользователей с использованием алгоритма Time-based one-time password (TOTP). Вы можете включить или выключить двухфакторную аутентификацию для всех пользователей. Двухфакторную аутентификацию также можно включить или выключить при создании и изменении локальных пользователей, LDAP-пользователей и LDAP-групп.

Если двухфакторная аутентификация включена для пользователя, при следующем входе пользователя в веб-интерфейс оркестратора генерируется уникальный QR-код. Пользователю нужно отсканировать QR-код с помощью программного или аппаратного аутентификатора, поддерживающего стандарт RFC 6238, например Kaspersky Password Manager, Google Authenticator, Яндекс Ключ и Microsoft Authenticator. Аутентификатор генерирует уникальный код, который пользователю нужно ввести, чтобы пройти двухфакторную аутентификацию и войти в веб-интерфейс оркестратора. Если пользователь вводит уникальный код неправильно более пяти раз, этот пользователь блокируется на 30 минут.

После прохождения двухфакторной аутентификации при входе в веб-интерфейс оркестратора пользователю нужно вводить имя пользователя, пароль и уникальный код. При необходимости вы можете повторно выполнить двухфакторную аутентификацию пользователя.

> Если время на оркестраторе и аутентификаторе отличается более чем на 30 секунд, возможны сбои при выполнении двухфакторной аутентификации пользователей. Мы рекомендуем синхронизировать время на оркестраторе и аутентификаторе с помощью NTP-сервера.

Права доступа

При необходимости вы можете создавать права доступа, определяющие, какие разделы и подразделы веб-интерфейса оркестратора, а также какие действия доступны пользователям, и назначать права доступа при создании и изменении пользователей и групп LDAP-пользователей. Например, вы можете создать право доступа, запрещающее переходить в раздел **Каталог** и создавать шаблоны сетевых сервисов.

По умолчанию пользователям и группам LDAP-пользователей назначается право доступа **Full Access**, которое предоставляет полный доступ ко всем функциям решения.

Запросы на подтверждение

При создании или изменении пользователя вам нужно указать, требуется ли автоматически создавать запрос на подтверждение, когда этот пользователь выполняет действие. Запросы на подтверждение можно подтвердить, отклонить или удалить. При подтверждении запроса выполняется связанное с ним действие. Отклоненные запросы на подтверждение сохраняются в веб-интерфейсе оркестратора.

Пользовательские сеансы

Для управления пользовательскими сеансами используются следующие функции:

- Ограничение продолжительности пользовательских сеансов. Если пользователь бездействует в течение 3600 секунд (одного часа) после входа в веб-интерфейс оркестратора, пользовательский сеанс автоматически прекращается. Вы можете указать вручную время бездействия до автоматического выхода.

- Завершение пользовательских сеансов. Если несколько сотрудников используют учетные данные одного пользователя для входа в веб-интерфейс оркестратора, любой из них может завершить другие пользовательские сеансы.

Работа с правами доступа

Вы можете посмотреть список прав доступа в разделе **Пользователи** на вкладке **Права доступа**. По умолчанию создано право доступа **Full access**, которое предоставляет полный доступ к веб-интерфейсу оркестратора и автоматически назначается пользователям и группам LDAP-пользователей, если вы не назначаете им другое право доступа.

Действия, которые вы можете выполнить со списком, описаны в инструкции Работа с таблицами компонентов решения.

Создание права доступа

Чтобы создать право доступа:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Права доступа**.

   Отобразится список прав доступа.

3. В верхней части списка нажмите на кнопку **+ Право доступа**.

4. В отобразившейся области настройки в поле **Имя** введите имя права доступа. Максимальная длина имени: 250 символов.

5. В блоке **Права доступа** рядом с разделами и подразделами веб-интерфейса оркестратора выберите одно из следующих значений:

   - **Изменение** – пользователи могут просматривать раздел или подраздел и выполнять в нем все доступные задачи.
   - **Просмотр** – пользователи могут только просматривать раздел или подраздел.
   - **Нет доступа** – пользователи не могут просматривать раздел или подраздел.

   Если вы хотите, чтобы подразделы наследовали значение, выбранное для раздела, установите флажок **Применить к подразделам**. Этот флажок снят по умолчанию.

6. Нажмите на кнопку **Создать**.

Право доступа будет создано и отобразится в списке.

Вы можете назначить право доступа при создании и изменении пользователя, а также при создании и изменении группы LDAP-пользователей.

Изменение права доступа

Чтобы изменить право доступа:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Права доступа**.

   Отобразится список прав доступа.

3. Нажмите на право доступа, которое вы хотите изменить.

4. В отобразившейся области настройки при необходимости измените следующие параметры:

   - имя права доступа;
   - разделы и подразделы веб-интерфейса оркестратора, а также действия, доступные пользователям.

5. Нажмите на кнопку **Сохранить**.

Право доступа будет изменено и обновится в списке.

Клонирование права доступа

Вы можете клонировать право доступа, чтобы создать такое же право доступа с другим именем.

Чтобы клонировать право доступа:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Права доступа**.

   Отобразится список прав доступа.

3. Нажмите на право доступа, которое вы хотите клонировать.

4. В верхней части отобразившейся области настройки нажмите на кнопку **Управление** → **Клонировать**.

5. В открывшемся окне введите имя нового права доступа.

6. Нажмите на кнопку **Клонировать**.

Клон права доступа с новым именем будет создан и отобразится в списке.

Удаление права доступа

Удаленные права доступа невозможно восстановить.

Чтобы удалить право доступа:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Права доступа**.

   Отобразится список прав доступа.

3. Нажмите на право доступа, которое вы хотите удалить.

4. В верхней части отобразившейся области настройки нажмите на кнопку **Управление** → **Удалить**.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Право доступа будет удалено и перестанет отображаться в списке.

Работа с LDAP-подключениями

Вы можете посмотреть таблицу LDAP-подключений в разделе **Пользователи** на вкладке **LDAP-подключения**. Информация о LDAP-подключениях отображается в следующих столбцах таблицы:

- **Имя** – имя LDAP-подключения.
- **Тип** – тип подключения. В этом столбце всегда отображается значение **LDAP**.
- **Хост** – имя хоста удаленного сервера.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание LDAP-подключения

Если вы хотите, чтобы LDAP-пользователи или группы LDAP-пользователей могли войти в веб-интерфейс оркестратора, используя свои учетные данные, вам нужно создать LDAP-подключение, с помощью которого оркестратор подключается к удаленному серверу, после чего перейти к созданию LDAP-пользователей или групп LDAP-пользователей.

Чтобы создать LDAP-подключение:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **LDAP-подключения**.

   Отобразится таблица LDAP-подключений.

3. Нажмите на кнопку **+ LDAP**.

4. В отобразившейся области настройки в поле **Имя** введите имя LDAP-подключения.

5. В поле **Домен** введите FQDN домена удаленного сервера.

6. В поле **Псевдоним домена** введите альтернативное имя или NETBIOS-имя домена. Пользователи вводят альтернативное имя, NETBIOS-имя или FQDN домена при входе в веб-интерфейс оркестратора.

   Например, если FQDN домена – example.com, а альтернативное имя – example, пользователь с именем admin может ввести следующие учетные данные при входе в веб-интерфейс оркестратора:

   - `admin@example.com`;
   - `admin@example`;
   - `example.com\admin`;
   - `example\admin`.

7. В поле **LDAP-хост** введите имя хоста удаленного сервера. Поддерживаются следующие форматы имени хоста:

   - `ldap://<имя хоста>:<номер порта>` – стандартный LDAP-сервер. Порт по умолчанию: 389.
   - `ldaps://<имя хоста>:<номер порта>` – LDAP-сервер с SSL-аутентификацией. Порт по умолчанию: 636.

   Например, если вы вводите `ldap://example.com:100`, имя хоста удаленного сервера – example.com, а номер порта – 100.

8. В поле **Базовое различающееся имя** введите базовое различающееся имя (англ. base distinguished name), которое оркестратор использует как начальную точку поиска учетных записей пользователей в директории удаленного сервера. Поддерживаются следующие форматы базового различающегося имени:

   - Для поиска в OpenLDAP введите базовое различающееся имя в формате `OU=<значение>,OU=<значение>`, где `OU` – структура организационных единиц в директории удаленного сервера. Например, если вы вводите `OU=OU_example1,OU=OU_example2`, начальной точкой поиска учетных записей пользователей является организационная единица OU_example2, находящаяся внутри OU_example1.
   - Для поиска в Microsoft Active Directory введите базовое различающееся имя в формате `DC=<значение>,DC=<значение>`, где `DC` – компоненты домена удаленного сервера. Например, если вы вводите `DC=example,DC=com`, начальной точкой поиска учетных записей пользователей является домен example.com.

9. В раскрывающемся списке **Атрибут поиска** выберите атрибут, который оркестратор использует для поиска учетных записей пользователей в директории удаленного сервера:

   - **uid (OpenLDAP)** – идентификатор пользователя UID (user ID) для поиска в OpenLDAP. Это значение выбрано по умолчанию.
   - **sAMAccountName (Active Directory)** – pre-Windows 2000 имя пользователя (англ. pre-Windows 2000 logon name) для поиска в Microsoft Active Directory.

10. В поле **Различающееся имя** введите различающееся имя (англ. distinguished name) для аутентификации оркестратора в удаленном сервере. Поддерживаются следующие форматы различающегося имени:

    - Для аутентификации в openLDAP введите значение в формате `UID=<значение>,OU=<значение>`, где `UID` – идентификатор пользователя, а `OU` – структура организационных единиц в директории удаленного сервера, в которой находится пользователь. Например, если вы вводите `UID=user_example,OU=OU_example`, для аутентификации оркестратора в удаленном сервере используется пользователь с идентификатором user_example, который находится в организационной единице OU_example.

    - Для аутентификации в Microsoft Active Directory введите значение в формате `CN=<значение>,OU=<значение>,DC=<значение>,DC=<значение>`, где `CN` – общее имя (англ. common name) пользователя, `OU` – структура организационных единиц в директории удаленного сервера, в которой находится пользователь, а `DC` – компоненты домена пользователя. Например, если вы вводите `CN=user_example,OU=OU_example,DC=example,DC=com`, для аутентификации оркестратора в удаленном сервере используется пользователь с именем user_example, который находится в организационной единице OU_example в домене example.com.

11. В поле **Пароль привязки** введите пароль удаленного сервера для аутентификации оркестратора в удаленном сервере. Вы можете посмотреть введенный пароль, нажав на значок просмотра 👁.

12. Если вы хотите убедиться в доступности удаленного сервера, нажмите на кнопку **Проверить аутентификацию**.

13. Нажмите на кнопку **Создать**.

    LDAP-подключение будет создано и отобразится в таблице.

Изменение LDAP-подключения

Чтобы изменить LDAP-подключение:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **LDAP-подключения**.

   Отобразится таблица LDAP-подключений.

3. Нажмите на LDAP-подключение, которое вы хотите изменить.

4. В отобразившейся области настройки при необходимости измените параметры LDAP-подключения. Описание параметров см. в инструкции по созданию LDAP-подключения.

5. Нажмите на кнопку **Сохранить**.

   LDAP-подключение будет изменено и обновится в таблице.

Изменение пароля LDAP-подключения

Вы можете изменить пароль удаленного сервера, указанный при создании LDAP-подключения, чтобы оркестратор использовал новый пароль для аутентификации в удаленном сервере.

Чтобы изменить пароль LDAP-подключения:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **LDAP-подключения**.

   Отобразится таблица LDAP-подключений.

3. Нажмите на LDAP-подключение, пароль которого вы хотите изменить.

4. В верхней части отобразившейся области настройки нажмите на кнопку **Управление** → **Изменить пароль**.

5. В открывшемся окне в полях **Новый пароль** и **Подтверждение пароля** введите новый пароль.

6. Нажмите на кнопку **Сохранить**.

Пароль LDAP-подключения будет изменен.

Удаление LDAP-подключения

Удаленные LDAP-подключения невозможно восстановить.

Чтобы удалить LDAP-подключение:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **LDAP-подключения**.

   Отобразится таблица LDAP-подключений.

3. Нажмите на LDAP-подключение, которое вы хотите удалить.

4. В верхней части отобразившейся области настройки нажмите на кнопку **Управление** → **Удалить**.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

LDAP-подключение будет удалено и перестанет отображаться в таблице.

Работа с пользователями

Вы можете посмотреть таблицу пользователей в разделе **Пользователи**. Информация о пользователях отображается в следующих столбцах таблицы:

- **Имя** – имя пользователя.
- **Тенант** – тенант, которому назначен пользователь.
- **Роль** – роль пользователя:
  - **Администратор**.
  - **Тенант**.
- **Источник** – тип пользователя:
  - **Локальный** – локальный пользователь.
  - **LDAP** – LDAP-пользователь.
- **Группа** – группа LDAP-пользователя. Если пользователь является локальным, в этом столбце отображается **Default**.
- **Состояние** – состояние пользователя:
  - **В сети**.
  - **Не в сети**.
  - **Заблокирован**.
- **Двухфакторная аутентификация** – двухфакторная аутентификация пользователя:
  - **Включено** – для пользователя включена двухфакторная аутентификация.
  - **Выключено** – для пользователя выключена двухфакторная аутентификация.
  - **Повторная инициализация** – для пользователя выполняется повторная двухфакторная аутентификация.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание пользователя

Вы можете создавать локальных и LDAP-пользователей. Учетные данные локальных пользователей хранятся в базе данных оркестратора. Учетные данные LDAP-пользователей хранятся на удаленном сервере. Если вы хотите, чтобы LDAP-пользователи могли войти в веб-интерфейс оркестратора, используя свои учетные данные, вам нужно создать LDAP-подключение, с помощью которого оркестратор подключается к удаленному серверу, после чего перейти к созданию LDAP-пользователей.

Чтобы создать пользователя:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Нажмите на кнопку **+ Пользователь**.

3. В отобразившейся области настройки в раскрывающемся списке **Тип учетной записи** выберите тип пользователя:

   - **Локальный**. Это значение выбрано по умолчанию. При выборе этого значения в полях **Пароль** и **Подтверждение пароля** введите пароль пользователя. Пароль должен содержать как минимум одну прописную букву латинского алфавита (A–Z), одну строчную букву (a–z), одну цифру и один специальный символ. Длина пароля: от 8 до 50 символов. Вы можете просмотреть введенный пароль, нажав на значок просмотра 👁.

   - **LDAP**.

   - **Сервис**.

4. В поле **Имя пользователя** введите имя пользователя. Формат имени пользователя на удаленном сервере: `user@domain` или `domain\user`.

5. В раскрывающемся списке **Роль** выберите роль пользователя:

   - **Администратор**.

   - **Тенант**.

   - **Ограничен-API-внешних-СЗИ**.

     Эта роль используется для интеграции Kaspersky SD-WAN с внешними средствами защиты информации через API оркестратора.

6. В раскрывающемся списке **Права доступа** выберите созданное право доступа, которое вы хотите назначить пользователю. По умолчанию пользователю назначается право доступа **Full access**, которое предоставляет полный доступ к веб-интерфейсу оркестратора.

7. Если вы хотите включить двухфакторную аутентификацию для пользователя, установите флажок **Двухфакторная аутентификация**. Этот флажок снят по умолчанию. При следующем входе в веб-интерфейс оркестратора пользователю нужно будет пройти двухфакторную аутентификацию.

   Вы не можете включить двухфакторную аутентификацию для отдельного пользователя, если двухфакторная аутентификация выключена для всех пользователей.

8. Если вы хотите, чтобы при каждом действии пользователя создавался запрос на подтверждение, установите флажок **Требуется подтверждение запроса**. Этот флажок снят по умолчанию, и пользователь может выполнять действия без подтверждения.

9. В поле **Имя** введите имя сотрудника.

10. В поле **Фамилия** введите фамилию сотрудника.

11. При необходимости укажите дополнительную информацию о пользователе:

    a. В поле **Эл. почта** введите адрес электронной почты.

    b. В поле **Описание** введите краткое описание пользователя.

12. Нажмите на кнопку **Создать**.

Пользователь будет создан и отобразится в таблице. По умолчанию пользователь заблокирован.

Вам нужно разблокировать пользователя, чтобы предоставить пользователю доступ к веб-интерфейсу оркестратора.

Разблокировка и блокировка пользователя

По умолчанию созданные пользователи заблокированы. Вам нужно разблокировать пользователя, чтобы предоставить пользователю доступ к веб-интерфейсу оркестратора.

Чтобы разблокировать или заблокировать пользователя:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Нажмите на пользователя, которого вы хотите разблокировать или заблокировать.

3. В верхней части отобразившейся области настройки нажмите на кнопку **Управление** → **Разблокировать** или **Заблокировать**.

Пользователь будет разблокирован или заблокирован.

Изменение пользователя

Вы не можете изменить тип и имя пользователя. Изменение пароля локального пользователя описано в отдельной инструкции.

Чтобы изменить пользователя:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Нажмите на пользователя, которого вы хотите изменить.

3. В отобразившейся области настройки при необходимости измените параметры пользователя. Описание параметров см. в инструкции по созданию пользователя.

4. Нажмите на кнопку **Сохранить**.

Пользователь будет изменен и обновится в таблице.

Изменение пароля локального пользователя

Пароли LDAP-пользователей хранятся на удаленных серверах, и их невозможно изменить в веб-интерфейсе оркестратора.

Чтобы изменить пароль локального пользователя:

1. Перейдите к изменению пароля локального пользователя:

   - Если вам назначена роль администратора платформы, и вы хотите изменить пароль созданного локального пользователя, в меню перейдите в раздел **Пользователи**, нажмите на локального пользователя и нажмите на кнопку **Управление** → **Изменить пароль**.

   - Если вам назначена роль тенанта, и вы хотите изменить свой пароль, в нижней части меню нажмите на значок настройки → **Изменить пароль**.

2. В открывшемся окне в полях **Новый пароль** и **Подтверждение пароля** введите новый пароль. Пароль должен содержать как минимум одну прописную букву латинского алфавита (A–Z), одну строчную букву (a–z), одну цифру и один специальный символ. Длина пароля: от 8 до 50 символов. Вы можете посмотреть введенный пароль, нажав на значок просмотра.

3. Нажмите на кнопку **Сохранить**.

Пароль локального пользователя будет изменен.

Повторная двухфакторная аутентификация пользователя

Вы можете выполнить повторную двухфакторную аутентификацию пользователя, если пользователь утратил доступ к сгенерированному при предыдущей двухфакторной аутентификации уникальному коду для входа в веб-интерфейс оркестратора.

Чтобы выполнить повторную аутентификацию пользователя:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Нажмите на пользователя, для которого вы хотите выполнить повторную двухфакторную аутентификацию.

3. В верхней части отобразившейся области настройки нажмите на кнопку **Управление** → **Перезапустить 2FA**.

При следующем входе в веб-интерфейс оркестратора пользователю нужно будет пройти двухфакторную аутентификацию.

Удаление пользователя

Удаленных пользователей невозможно восстановить.

Чтобы удалить пользователя:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Нажмите на пользователя, которого вы хотите удалить.

3. В верхней части отобразившейся области настройки нажмите на кнопку **Управление** → **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Пользователь будет удален и перестанет отображаться в таблице.

Работа с группами LDAP-пользователей

Вы можете посмотреть таблицу групп LDAP-пользователей в разделе **Пользователи** на вкладке **Группы**. Информация о группах LDAP-пользователей отображается в следующих столбцах таблицы:

- **Имя** – имя группы LDAP-пользователей.
- **Тенант** – тенант, которому назначена группа LDAP-пользователей.
- **Роль** – роль LDAP-пользователей.
- **Тип** – тип группы пользователей. Kaspersky SD-WAN поддерживает только группы LDAP-пользователей.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание группы LDAP-пользователей

Учетные данные групп LDAP-пользователей хранятся на удаленном сервере. Если вы хотите, чтобы группа LDAP-пользователей могла войти в веб-интерфейс оркестратора, используя свои учетные данные, вам нужно создать LDAP-подключение, с помощью которого оркестратор подключается к удаленному серверу, после чего перейти к созданию группы LDAP-пользователей.

Если пользователь состоит в нескольких группах LDAP-пользователей на удаленном сервере, мы рекомендуем создать только одну из групп LDAP-пользователей в веб-интерфейсе оркестратора. Если в веб-интерфейсе оркестратора создано несколько групп LDAP-пользователей, пользователь, являющийся участником всех этих групп LDAP-пользователей, входит в веб-интерфейс оркестратора как участник группы LDAP-пользователей, которая была создана раньше всех остальных.

Чтобы создать группу LDAP-пользователей:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Группы**.

   Отобразится таблица групп LDAP-пользователей.

3. Нажмите на кнопку **+ Группа пользователей**.

4. В отобразившейся области настройки в поле **Имя** введите имя группы LDAP-пользователей на удаленном сервере в формате `user@domain` или `domain\user`.

5. В раскрывающемся списке **Роль** выберите роль LDAP-пользователей в группе:

   - **Администратор**.
   - **Тенант**.

6. В раскрывающемся списке **Права доступа** выберите созданное право доступа, которое вы хотите назначить группе LDAP-пользователей. По умолчанию группе LDAP-пользователей назначается право доступа **Full access**, которое предоставляет полный доступ к веб-интерфейсу оркестратора.

7. Если вы хотите включить двухфакторную аутентификацию для группы LDAP-пользователей, установите флажок **Двухфакторная аутентификация**. Этот флажок снят по умолчанию. При следующем входе в веб-интерфейс оркестратора пользователям LDAP-группы нужно будет пройти двухфакторную аутентификацию.

   Когда двухфакторная аутентификация включена для группы LDAP-пользователей, прошедшие двухфакторную аутентификацию LDAP-пользователи отображаются в таблице пользователей. Вы можете выключить двухфакторную аутентификацию для LDAP-пользователя при изменении этого пользователя.

   Вы не можете включить двухфакторную аутентификацию для группы LDAP-пользователей, если двухфакторная аутентификация выключена для всех пользователей.

8. Нажмите на кнопку **Создать**.

Группа LDAP-пользователей будет создана и отобразится в таблице.

Изменение группы LDAP-пользователей

Вы не можете изменить тип и имя группы LDAP-пользователей.

Чтобы изменить группу пользователей:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Группы**.

   Отобразится таблица групп LDAP-пользователей.

3. Нажмите на группу LDAP-пользователей, которую вы хотите изменить.

4. В отобразившейся области настройки при необходимости измените параметры группы LDAP-пользователей. Описание параметров см. в инструкции по созданию группы LDAP-пользователей.

5. Нажмите на кнопку **Сохранить**.

Группа LDAP-пользователей будет изменена и обновится в таблице.

Удаление группы LDAP-пользователей

Удаленные группы LDAP-пользователей невозможно восстановить.

Чтобы удалить группу LDAP-пользователей:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Группы**.

   Отобразится таблица групп LDAP-пользователей.

3. Нажмите на группу LDAP-пользователей, которую вы хотите удалить.

4. В верхней части отобразившейся области настройки нажмите на кнопку **Управление** → **Удалить**.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Группа LDAP-пользователей будет удалена и перестанет отображаться в таблице.

Включение и выключение двухфакторной аутентификации для всех пользователей

Вы можете включить или выключить двухфакторную аутентификацию для всех пользователей. Если двухфакторная аутентификация выключена для всех пользователей, вы не можете включить ее для локальных и LDAP-пользователей, а также для групп LDAP-пользователей. По умолчанию двухфакторная аутентификация выключена.

Чтобы включить или выключить двухфакторную аутентификацию для всех пользователей:

1. В меню перейдите в раздел **Пользователи**.

   Отобразится страница управления пользователями. По умолчанию выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Двухфакторная аутентификация**.

3. Выполните одно из следующих действий:

   - Если вы хотите включить двухфакторную аутентификацию для всех пользователей, установите флажок **Двухфакторная аутентификация для всех пользователей**. При следующем входе в веб-интерфейс оркестратора всем пользователям нужно будет пройти двухфакторную аутентификацию.

   - Если вы хотите выключить двухфакторную аутентификацию для всех пользователей, снимите флажок **Двухфакторная аутентификация для всех пользователей**.

   Этот флажок установлен по умолчанию.

Двухфакторная аутентификация будет включена или выключена для всех пользователей.

Работа с запросами на подтверждение

Если при создании или изменении пользователя вы установили флажок **Требуется подтверждение запроса**, при каждом действии пользователя автоматически создается запрос на подтверждение. Вы можете подтвердить, отклонить и удалить запрос на подтверждение. При подтверждении запроса происходит выполнение связанного с ним действия, а отклоненный запрос сохраняется в веб-интерфейсе оркестратора.

Чтобы подтвердить, отклонить или удалить запрос на подтверждение:

1. В меню перейдите в раздел **Подтверждение**.

   Отобразится таблица запросов на подтверждение. Информация о запросах на подтверждение отображается в следующих столбцах таблицы:

   - **Метод** – метод API, который был использован для создания запроса на подтверждение.
   - **URL** – веб-адрес API.
   - **Подсказка** – краткое описание запроса на подтверждение.
   - **Пользователь** – имя пользователя, действие которого привело к созданию запроса на подтверждение.
   - **Заголовки** – заголовки API.
   - **Создан** – дата и время создания запроса на подтверждение.
   - **Статус** – статус выполнения запроса на подтверждение:
     - **Подтверждено**.
     - **Отклонено**.
     - **Ошибка**.
     - **Ожидание подтверждения**.

   Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

2. При необходимости выполните одно из следующих действий:

   - Для подтверждения запроса нажмите рядом с ним на кнопку **Разрешить**.
   - Для отклонения запроса нажмите рядом с ним на кнопку **Отклонить**.
   - Для удаления запроса нажмите рядом с ним на кнопку **Удалить**.

   Если вы хотите подтвердить, отклонить или удалить несколько запросов на подтверждение одновременно, установите флажки рядом с запросами и выберите действие, нажав на кнопку **Действие** в верхней части таблицы.

Запросы на подтверждение будут подтверждены, отклонены или удалены.

Работа с пользовательскими сеансами

Вы можете выполнять следующие действия с пользовательскими сеансами:

- Ограничить продолжительность пользовательских сеансов. По умолчанию если пользователь бездействует на протяжении 3600 секунд (одного часа) после входа в веб-интерфейс оркестратора, пользовательский сеанс прекращается.
- Посмотреть и при необходимости завершить активные пользовательские сеансы.

Чтобы работать с пользовательскими сеансами:

1. В меню перейдите в раздел **Система**.

   По умолчанию выбрана вкладка **Мониторинг**, на которой отображаются параметры подключения к серверу Zabbix.

2. Выберите вкладку **Пользовательские сеансы**.

   Отобразится таблица пользовательских сеансов. Информация о пользовательских сеансах отображается в следующих столбцах таблицы:

   - **IP-адрес** – IP-адрес пользователя.
   - **Пользовательский агент** – информация о браузере и оперативной системе пользователя.
   - **Дата** – дата начала пользовательского сеанса.

   Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

3. При необходимости выполните одно из следующих действий:

   - Если вы хотите ограничить продолжительность пользовательских сеансов в поле **При бездействии заканчивать сеанс после (сек.)** введите время в секундах, по истечении которого пользовательский сеанс прекращается при бездействии. Диапазон значений: от 60 до 86 400. Значение по умолчанию: `3600`.
   - Если вы хотите завершить отдельный пользовательский сеанс, нажмите рядом с ним на кнопку **Закончить сеанс**.
   - Если вы хотите завершить несколько пользовательских сеансов, установите рядом с ними флажки и в верхней части таблицы нажмите на кнопку **Действия → Закончить сеанс**.

4. Нажмите на кнопку **Сохранить**.

Мультитенантность

Вы можете развернуть Kaspersky SD-WAN для нескольких *тенантов*, которые могут быть независимыми клиентами, а также офисами или подразделениями вашей организации. Решение, развернутое для тенанта, называется *экземпляром SD-WAN*. После развертывания решения вам нужно создать хотя бы одного тенанта и развернуть для него экземпляр SD-WAN.

Когда вы создаете тенанта, ему становится доступным собственный портал самообслуживания для управления экземпляром SD-WAN. Созданные тенанты изолированы, поэтому они не могут получить доступ к порталам самообслуживания друг-друга и могут использовать пересекающиеся IP-сети. Количество созданных тенантов не должно превышать количество тенантов, которых вы указали в блоке `external` конфигурационного файла при развертывании решения.

Для развертывания экземпляра SD-WAN для тенанта вам нужно создать шаблон экземпляра SD-WAN. В шаблоне экземпляра SD-WAN необходимо указать основные параметры экземпляра SD-WAN, например параметры качества обслуживания и транспортных сервисов. Вам также нужно добавить тенанта в шаблон экземпляра SD-WAN, чтобы при развертывании экземпляра SD-WAN для тенанта к экземпляру SD-WAN были применены параметры шаблона экземпляра SD-WAN.

Если тенант не добавлен ни в один шаблон экземпляра SD-WAN, при развертывании экземпляра SD-WAN для тенанта используется шаблон экземпляра SD-WAN по умолчанию **Default SD-WAN template**. Вы можете назначить другой шаблон экземпляра SD-WAN по умолчанию.

Если параметры, которые вы указали в шаблоне экземпляра SD-WAN, не совпадают с фактическими параметрами экземпляра SD-WAN, экземпляр SD-WAN не развертывается для тенанта. Например, экземпляр SD-WAN не развертывается, если количество узлов контроллера, указанное в шаблоне экземпляра SD-WAN, не совпадает с реальным количеством узлов контроллера экземпляра SD-WAN.

После развертывания экземпляра SD-WAN вы можете просматривать результаты мониторинга и сервисные запросы, а также настраивать узлы контроллера экземпляра SD-WAN. В развернутый экземпляр SD-WAN можно добавить тенантов, чтобы они использовали контроллер экземпляра SD-WAN. Это позволяет не развертывать отдельный экземпляр SD-WAN для каждого тенанта.

Экземпляры SD-WAN можно сгруппировать в пулы экземпляров SD-WAN для балансировки нагрузки при использовании большого количества устройств CPE. Вы можете добавить устройства CPE в пул экземпляров SD-WAN. Если вы добавили устройство CPE в пул экземпляров SD-WAN, оркестратор автоматически выбирает экземпляр SD-WAN с наименьшим количеством устройств CPE и добавляет экземпляру SD-WAN устройство CPE. Если экземплярам SD-WAN в пуле экземпляров SD-WAN добавлено одинаковое количество устройств CPE, оркестратор добавляет устройство CPE случайному экземпляру SD-WAN.

Сценарий: развертывание экземпляра SD-WAN для тенанта

Сценарий развертывания экземпляра SD-WAN для тенанта состоит из следующих этапов:

1. **Создание тенанта**

   Создайте тенанта, для которого вы хотите развернуть экземпляр SD-WAN.

2. **Создание шаблона экземпляра SD-WAN**

Создайте и настройте шаблон экземпляра SD-WAN. Более подробно о работе с шаблонами экземпляра SD-WAN см. в разделе Работа с шаблонами экземпляра SD-WAN. Вы можете использовать созданный шаблон экземпляра SD-WAN для развертывания других экземпляров SD-WAN.

3. **Добавление тенанта в шаблон экземпляра SD-WAN**

   Добавьте тенанта в шаблон экземпляра SD-WAN, чтобы при развертывании экземпляра SD-WAN для тенанта к экземпляру SD-WAN были применены параметры шаблона экземпляра SD-WAN.

4. **Подготовка виртуальных машин или физических серверов для развертывания контроллера**

   При развертывании Kaspersky SD-WAN вы подготовили виртуальные машины или физические сервера для развертывания всех компонентов решения, включая контроллер.

   Если вы не подготовили виртуальные машины или физические сервера для контроллера, вы можете указать их в блоке `nodes` конфигурационного файла, после чего заново выполнить команду развертывания решения. При повторном выполнении команды развертывания решения будут подготовлены недостающие виртуальные машины или физические сервера. Работа уже развернутых компонентов решения затронута не будет.

5. **Подготовка пакета PNF контроллера**

   Подготовьте пакет PNF контроллера экземпляра SD-WAN на локальном устройстве:

   1. Распакуйте архив установки и перейдите в одну из следующих директорий:

      - Если вы хотите развернуть один узел контроллера, перейдите в директорию /pnfs/pnf_sdwan_ctl.
      - Если вы хотите развернуть три узла контроллера, перейдите в директорию /pnfs/pnf_sdwan_ctl_3.
      - Если вы хотите развернуть пять узлов контроллера, перейдите в директорию /pnfs/pnf_sdwan_ctl_5.

   2. При необходимости изменить PNF-дескриптор контроллера перейдите в директорию /src распакованного архива установки и измените файл pnfd.xml.

   3. Создайте пакет PNF, выполнив команду:

      ```
      make
      ```

   Пакет PNF будет помещен в директорию /build распакованного архива установки.

6. **Загрузка пакета PNF контроллера в веб-интерфейс оркестратора**

   Загрузите в веб-интерфейс оркестратора пакет PNF контроллера экземпляра SD-WAN.

7. **Настройка PNF контроллера**

   Настройте PNF контроллера экземпляра SD-WAN:

   1. В меню перейдите в раздел **Каталог** и в панели **Каталог** нажмите на PNF контроллера.

   2. В отобразившейся области настройки выберите вкладку **Размещение в ЦОД** и в поле **Центр обработки данных** укажите добавленный центр обработки данных, в котором вы хотите развернуть контроллер.

   3. Выберите вкладку **Управляющий IP** и укажите IP-адреса узлов контроллера. Вам нужно указать стандартные или виртуальные IP-адреса виртуальных машин или физических серверов для развертывания контроллера, которые вы указали в блоке `nodes` конфигурационного файла при развертывании решения.

8. **Назначение PNF контроллера тенанту**

Назначьте PNF контроллера экземпляра SD-WAN тенанту.

9. **Вход на портал самообслуживания тенанта**

   Войдите на портал самообслуживания тенанта.

10. **Создание сетевого сервиса SD-WAN**

    Создайте сетевой сервис SD-WAN. При создании сетевого сервиса SD-WAN вам нужно добавить в топологию PNF контроллера экземпляра SD-WAN, после чего выполнить следующие действия:

    1. В топологии нажмите на PNF контроллера.
    2. В отобразившейся области настройки выберите вкладку **CA_certificates** и в поле **CA certificate** введите корневой сертификат в формате PEM, которым подписан сертификат оркестратора. Поддерживаются одиночные корневые сертификаты и цепочки сертификатов, состоящие из одного корневого сертификата и нескольких промежуточных сертификатов. Если вы указываете цепочку сертификатов, вам нужно начинать каждый сертификат с новой строки.
    3. Выберите вкладку **Orchestrator** и в поле **Orchestrator's API IP** введите IP-адрес одного из узлов оркестратора. Вам нужно указать один из стандартных или виртуальных IP-адресов виртуальных машин или физических серверов для развертывания оркестратора, которые вы указали в блоке `nodes` конфигурационного файла.
    4. Выберите вкладки **CTL1–5** и укажите информацию об узлах контроллера:
       1. В поле **IP for ORC connection** введите IP-адрес узла контроллера для подключения оркестратора. Вам нужно указать один из стандартных или виртуальных IP-адресов виртуальных машин или физических серверов для развертывания контроллера, которые вы указали в блоке `nodes` конфигурационного файла.
       2. В поле **IP for CPE connections** введите IP-адрес узла контроллера для подключения устройств CPE.
       3. В поле **PORT for CPE connections** введите номер TCP-порта узла контроллера для подключения устройств CPE.

11. **Развертывание сетевого сервиса SD-WAN**

    Разверните сетевой сервис SD-WAN.

Экземпляр SD-WAN будет развернут для тенанта, и контроллер экземпляра SD-WAN отобразится на портале администратора и портале самообслуживания тенанта в разделе **Инфраструктура**.

Если на этапе 10 этого сценария вы указали неверный корневой сертификат, вам нужно выполнить следующие действия:

1. Подключитесь к виртуальной машине или физическому серверу, на котором развернут узел контроллера. Вместе с каждым узлом контроллера на виртуальной машине или физическом сервере автоматически разворачивается компонент MOCKPNF для обеспечения безопасности настройки Docker-контейнера узла контроллера.
2. Войдите в учетную запись пользователя, который имеет доступ к Docker-группе, после чего войдите в Docker-контейнер компонента MOCKPNF, выполнив команду:

   ```
   docker exec -it mockpnf-<номер узла контроллера> /bin/ash
   ```

3. Выполните скрипт `cleanup.sh`. Вы можете скачать скрипт из директории /pnfs/pnf_sdwan_ctl<количество узлов контроллера>/scr/scripts архива установки.

   > Вам нужно выполнить шаги 2–3 для каждого узла контроллера.

4. Повторно выполните этап 10 этого сценария, при этом указав правильный корневой сертификат.

Работа с тенантами

Вы можете посмотреть список тенантов в разделе **Тенанты**. В этом разделе также отображаются следующие блоки:

- **Группы пользователей** – позволяет назначить тенанту группы LDAP-пользователей. Назначенные группы LDAP-пользователей могут входить на портал самообслуживания тенанта и управлять экземпляром SD-WAN, который был развернут для тенанта.
- **VIM** – позволяет назначить тенанту VIM. Тенант может управлять виртуальными сетевыми функциями в рамках виртуальной инфраструктуры с помощью назначенных VIM.
- **Каталог** – позволяет назначить тенанту компоненты сетевого сервиса. Тенант может управлять сетевыми сервисами с помощью назначенных компонентов сетевого сервиса.
- **[[ten.sdwan.header]]** – позволяет посмотреть компоненты сетевого сервиса SD-WAN тенанта.
- **Ресурсы** – позволяет назначить тенанту вычислительные ресурсы. Назначенные вычислительные ресурсы определяют производительность экземпляра SD-WAN, который будет развернут для тенанта. Количество доступных вычислительных ресурсов определяется при развертывании решения.
- **Сервисные запросы** – позволяет посмотреть сервисные запросы тенанта.
- **Пользователи** – позволяет назначить тенанту пользователей. Назначенные пользователи могут входить на портал самообслуживания тенанта и управлять экземпляром SD-WAN, который был развернут для тенанта.
- **[[ten.cpe.header]]** – позволяет добавить тенанту устройства CPE. Тенант может передавать трафик между площадками с помощью добавленных устройств CPE.

Создание тенанта

Количество созданных тенантов не должно превышать количество тенантов, которых вы указали в блоке `external` конфигурационного файла при развертывании решения.

Чтобы создать тенанта:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.

2. Начните создание тенанта одним из следующих способов:

   - Если вы создаете первого тенанта в блоке **Тенанты** в поле **Имя** введите имя тенанта.
   - Если вы создаете второго или последующих тенантов, в верхней части блока **Тенанты** нажмите на кнопку **+ Тенант** и в поле **Имя** введите имя тенанта.

3. При необходимости в блоке в нижней части страницы введите краткое описание тенанта.

4. Нажмите на значок создания +.

Тенант будет создан и отобразится в блоке **Тенанты**.

Назначение тенанту пользователя

Вы можете назначить тенанту пользователей, чтобы пользователи могли входить на портал самообслуживания тенанта и управлять экземпляром SD-WAN, который был развернут для тенанта. Для назначения пользователя тенанту вам нужно предварительно назначить пользователю роль **Тенант** при создании или изменении пользователя. Вы можете назначить пользователя с ролью **Тенант** нескольким тенантам, и вы можете назначать каждому тенанту несколько пользователей с ролью **Тенант**.

Чтобы назначить тенанту пользователей:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.

2. Нажмите на имя тенанта, которому вы хотите назначить пользователей, или выберите его в таблице и нажмите на кнопку **Изменить тенант**.

   Откроется область изменения параметров тенанта.

3. Перейдите на вкладку **Пользователи** и включите переключатель **Использовать** для одного или нескольких пользователей, которых вы хотите назначить тенанту.

   Если вы хотите назначить тенанту все группы в таблице, нажмите на кнопку **Использовать все**.

Пользователи будут назначены тенанту. Тенант, которому были назначены пользователи, будет отображаться в меню **Пользователи** в таблице пользователей в столбце **Тенант**.

Назначение тенанту группы LDAP-пользователей

Вы можете назначить тенанту группы LDAP-пользователей, чтобы пользователи групп могли входить на портал самообслуживания тенанта и управлять экземпляром SD-WAN, который был развернут для тенанта. Для назначения группы LDAP-пользователей тенанту вам нужно предварительно назначить группе LDAP-пользователей роль **Тенант** при создании или изменении группы LDAP-пользователей. Вы можете назначить группу LDAP-пользователей с ролью **Тенант** нескольким тенантам, и вы можете назначать каждому тенанту несколько группу LDAP-пользователей с ролью **Тенант**.

Чтобы назначить тенанту группу LDAP-пользователей:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.

2. Нажмите на имя тенанта, которому вы хотите назначить группу LDAP-пользователей, или выберите его в таблице и нажмите на кнопку **Изменить тенант**.

   Откроется область изменения параметров тенанта.

3. Перейдите на вкладку **Группы пользователей** и включите переключатель **Использовать** для одной или нескольких групп LDAP-пользователей, которых вы хотите назначить тенанту.

   Если вы хотите назначить тенанту все группы в таблице, нажмите на кнопку **Использовать все**.

Группы LDAP-пользователей будут назначены тенанту. Тенант, которому были назначены группы LDAP-пользователей, будет отображаться в меню **Пользователи** → **Группы** в таблице групп в столбце **Тенант**.

Назначение тенанту вычислительных ресурсов

Вы можете назначить тенанту вычислительные ресурсы, чтобы определить производительность экземпляра SD-WAN, который вы развернете для тенанта. Количество доступных вычислительных ресурсов определяется при развертывании решения.

Чтобы назначить тенанту вычислительные ресурсы:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта, которому вы хотите назначить вычислительные ресурсы.

3. В верхней части блока **Ресурсы** нажмите на значок настройки ⚙.

4. Нажмите на значок изменения объема ∞ рядом с одним из следующих вычислительных ресурсов:

   - **ЦП** – виртуальные процессорные ядра.
   - **ОЗУ** – оперативная память.
   - **Диск** – дисковое пространство.

5. В отобразившемся поле введите объем вычислительного ресурса, который вы хотите назначить тенанту.
6. Нажмите на значок сохранения ✓.

Указанный объем вычислительных ресурсов будет назначен тенанту.

Назначение тенанту компонентов сетевого сервиса

Вы можете назначить тенанту компоненты сетевого сервиса, чтобы тенант управлял с их помощью сетевыми сервисами.

Чтобы назначить тенанту компоненты сетевого сервиса:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.
2. В блоке **Тенанты** выберите тенанта, которому вы хотите назначить компоненты сетевого сервиса.
3. В блоке **Каталог** установите флажки рядом с компонентами сетевого сервиса, которые вы хотите назначить тенанту.

Компоненты сетевого сервиса будут назначены тенанту и отобразятся в портале самообслуживания тенанта в разделе **Каталог**.

Назначение тенанту VIM

Вы можете назначить тенанту один или несколько VIM, чтобы тенант управлял с помощью этих VIM виртуальными сетевыми функциями в рамках виртуальной инфраструктуры.

Чтобы назначить VIM тенанту:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.
2. В блоке **Тенанты** выберите тенанта, которому вы хотите назначить VIM, и нажмите на кнопку **+ Изменить VIM**.

   Откроется область изменения параметров VIM тенанта.
3. На вкладке **Список** в таблице включите переключатель **Использовать** для одного или нескольких VIM, которых вы хотите назначить тенанту.
4. Вы можете отфильтровать список VIM с помощью выпадающих списков **Домен** и **Центр обработки данных**, выбрав в них созданный домен и добавленный центр обработки данных, в котором вы развернули VIM.

VIM будут назначены тенанту и отобразятся в таблице тенантов в столбце **VIM**.

Вход на портал самообслуживания тенанта

Чтобы войти на портал самообслуживания тенанта:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта, на портал самообслуживания которого вы хотите войти.

3. Нажмите на кнопку **Подключиться как тенант**.

Портал самообслуживания тенанта откроется в новой вкладке браузера. Вы войдете на портал самообслуживания.

Изменение тенанта

Чтобы изменить тенанта:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** нажмите на значок настройки ⚙ → **Изменить** рядом с тенантом, которого вы хотите изменить.

3. При необходимости измените имя и/или краткое описание тенанта.

4. Нажмите на значок сохранения ✓.

Тенант будет изменен и обновится в блоке **Тенанты**.

Удаление тенанта

Когда вы удаляете тенанта, автоматически удаляется развернутый для него экземпляр SD-WAN. При этом на портале администратора сохраняются все созданные в рамках тенанта объекты, например зоны и шаблоны межсетевого экрана.

Удаленных тенантов невозможно восстановить.

Чтобы удалить тенанта:

1. В меню перейдите в раздел **Тенанты**.

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** нажмите на значок настройки ⚙ → **Удалить** рядом с тенантом, которого вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Тенант будет удален и перестанет отображаться в блоке **Тенанты**.

Работа с шаблонами экземпляра SD-WAN

Вы можете посмотреть таблицу шаблонов экземпляра SD-WAN в разделе **SD-WAN → Шаблоны экземпляров SD-WAN**. По умолчанию создан шаблон экземпляра SD-WAN **Default SD-WAN template**. Информация о шаблонах экземпляра SD-WAN отображается в следующих столбцах таблицы:

- **ID** – идентификатор шаблона экземпляра SD-WAN.
- **Имя** – имя шаблона экземпляра SD-WAN.
- **Используется** – шаблон экземпляра SD-WAN используется экземплярами SD-WAN:
  - **Да**.
  - **Нет**.
- **Изменено** – дата и время последнего изменения параметров шаблона экземпляра SD-WAN.
- **Пользователь** – имя пользователя, который создал шаблон экземпляра SD-WAN.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Параметры шаблона экземпляра SD-WAN можно настроить на следующих вкладках:

- **Информация** – основная информация о шаблоне экземпляра SD-WAN. Вы можете изменить имя шаблона экземпляра SD-WAN в поле **Имя**.
- **Классы трафика** – параметры классов трафика.
- **Классификаторы** – параметры классификаторов трафика.
- **QoS-правила** – параметры правил качества обслуживания.
- **Транспортные сервисы** – параметры транспортных сервисов.
- **Тенанты** – тенанты, которые были добавлены в шаблон экземпляра SD-WAN.
- **Высокая доступность** – количество узлов контроллера экземпляра SD-WAN.
- **Транспортная/сервисная стратегия** – транспортная стратегия, используемая в экземпляре SD-WAN.

Создание шаблона экземпляра SD-WAN

Чтобы создать шаблон экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. В верхней части страницы нажмите на кнопку **+ [[common.add Добавить]]**.

3. В открывшемся окне введите имя шаблона экземпляра SD-WAN.

4. Нажмите на кнопку **Создать**.

   Шаблон экземпляра SD-WAN будет создан и отобразится в таблице.

Вам нужно настроить созданный шаблон экземпляра SD-WAN. В шаблоне экземпляра SD-WAN необходимо указать основные параметры экземпляра SD-WAN, например параметры качества обслуживания и транспортных сервисов. Вам также нужно добавить тенанта в шаблон экземпляра SD-WAN, чтобы при развертывании экземпляра SD-WAN для тенанта к экземпляру SD-WAN были применены параметры шаблона экземпляра SD-WAN. Более подробно о работе с шаблонами экземпляра SD-WAN см. в разделе Работа с шаблонами экземпляра SD-WAN.

Назначение шаблона экземпляра SD-WAN по умолчанию

Если тенант не добавлен ни в один шаблон экземпляра SD-WAN, при развертывании экземпляра SD-WAN для тенанта используется шаблон экземпляра SD-WAN по умолчанию **Default SD-WAN template**. Вы можете назначить другой шаблон экземпляра SD-WAN по умолчанию.

Чтобы назначить шаблон экземпляра SD-WAN по умолчанию:

1. В меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, который вы хотите назначить шаблоном экземпляра SD-WAN по умолчанию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Назначить шаблоном по умолчанию**.

Шаблон экземпляра SD-WAN будет назначен шаблоном экземпляра SD-WAN по умолчанию.

Выбор количества узлов контроллера экземпляра SD-WAN

Экземпляр SD-WAN не развертывается, если количество узлов контроллера, указанное в шаблоне экземпляра SD-WAN, не совпадает с реальным количеством узлов контроллера экземпляра SD-WAN.

Чтобы выбрать количество узлов контроллера экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN** → **Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, для которого вы хотите выбрать количество узлов контроллера.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. Выберите вкладку **Высокая доступность**.

4. Выберите количество узлов контроллера.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Добавление тенанта в шаблон экземпляра SD-WAN

Вам нужно добавить тенанта в шаблон экземпляра SD-WAN, чтобы при развертывании экземпляра SD-WAN для тенанта к экземпляру SD-WAN были применены параметры шаблона экземпляра SD-WAN.

Чтобы добавить тенанта в шаблон экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN** → **Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, в который вы хотите добавить тенанта.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. Выберите вкладку **Тенанты**.

   Отобразится таблица тенантов.

4. Нажмите на кнопку **+ Тенант**.

5. В открывшемся окне выберите созданного тенанта, которого вы хотите добавить в шаблон экземпляра SD-WAN.

6. Нажмите на кнопку **Добавить**.

   Тенант будет добавлен в шаблон экземпляра SD-WAN и отобразится в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Удаление тенанта из шаблона экземпляра SD-WAN

Вы можете удалить тенанта из шаблона экземпляра SD-WAN, чтобы при развертывании экземпляра SD-WAN для тенанта не использовался шаблон экземпляра SD-WAN.

Чтобы удалить тенанта из шаблона экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN** → **Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, из которого вы хотите удалить тенанта.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. Выберите вкладку **Тенанты**.

   Отобразится таблица тенантов.

4. Нажмите на кнопку **Удалить** рядом с тенантом, которого вы хотите удалить из шаблона экземпляра SD-WAN.

   Тенант будет удален из шаблона экземпляра SD-WAN и перестанет отображаться в таблице.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Удаление шаблона экземпляра SD-WAN

Вы не можете удалить шаблон экземпляра SD-WAN по умолчанию.

Удаленные шаблоны экземпляра SD-WAN невозможно восстановить.

Чтобы удалить шаблон экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN** → **Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, который вы хотите удалить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Шаблон экземпляра SD-WAN будет удален и перестанет отображаться в таблице.

Работа с экземплярами SD-WAN

Вы можете посмотреть таблицу экземпляров SD-WAN в разделе **SD-WAN → Экземпляры SD-WAN**. Информация об экземплярах SD-WAN отображается в следующих столбцах таблицы:

- **ID** – идентификатор экземпляра SD-WAN.
- **Тенант** – тенант, для которого развернут экземпляр SD-WAN.
- **Статус** – статус экземпляра SD-WAN:
  - **Ок** – экземпляр SD-WAN работает в штатном режиме.
  - **Контроллер отсутствует** – у экземпляра SD-WAN отсутствует контроллер.
  - **Ошибка** – при работе экземпляра SD-WAN возникла ошибка.
  - **Удаление** – экземпляр SD-WAN находится в процессе удаления.
  - **Удален** – экземпляр SD-WAN удален.
- **[[sdwan.cpeCount]]** – количество устройств CPE, которые были добавлены экземпляру SD-WAN.
- **Контроллеры** – IP-адреса и номера портов контроллеров экземпляра SD-WAN.
- **ЦОД** – центр обработки данных, в котором развернут экземпляр SD-WAN.
- **VIM** – VIM экземпляра SD-WAN.
- **Создан** – дата и время развертывания экземпляра SD-WAN.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Параметры экземпляра SD-WAN можно настроить на следующих вкладках:

- **Конфигурация** – основная информация об экземпляре SD-WAN и параметры узлов контроллера экземпляра SD-WAN. Вы можете ввести краткое описание экземпляра SD-WAN в поле **Описание**.
- **Мониторинг** – результаты мониторинга экземпляра SD-WAN.
- **Сервисные запросы** – сервисные запросы экземпляра SD-WAN.
- **Самообслуживание тенанта** – тенанты, которые были добавлены в экземпляр SD-WAN.

Настройка узлов контроллера экземпляра SD-WAN

При настройке узлов контроллера экземпляра SD-WAN вы можете изменить их IP-адреса и номера TCP-портов. В этом случае IP-адреса и номера TCP-портов узлов контроллера автоматически изменятся на всех устройствах CPE, которые добавлены экземпляру SD-WAN. Если интерфейсы SD-WAN с типом WAN устройства CPE подключены к разным сетям, например к интернету и частной MPLS-сети, вы можете изменить IP-адреса и номера TCP-портов узлов контроллера на отдельных интерфейсах SD-WAN с типом WAN при создании или изменении интерфейсов SD-WAN с типом WAN. IP-адреса и номера TCP-портов, указанные на отдельном интерфейсе SD-WAN с типом WAN, являются более приоритетными по отношению к IP-адресам и номерам TCP-портов, указанным при настройке узлов контроллера экземпляра SD-WAN.

Если при развертывании экземпляра SD-WAN вы развернули несколько узлов контроллера, при настройке узлов контроллера экземпляра SD-WAN вы можете указать, какой из них является узлом-арбитром. Когда узел-арбитр указан в веб-интерфейсе оркестратора, устройства CPE не устанавливают управляющие сессии с этим узлом контроллера, за счет чего снижается нагрузка на устройства CPE.

После настройки узлов контроллера экземпляра SD-WAN вам нужно перезагрузить уже зарегистрированные устройства CPE, чтобы изменения вступили в силу.

Чтобы настроить узлы контроллера экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN, узлы контроллера которого вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Конфигурация**, на которой отображается основная информация об экземпляре SD-WAN.

3. При необходимости выполните одно из следующих действий:

   - Если вы хотите изменить IP-адрес узла контроллера, в поле **IP-адрес** введите IPv4-адрес. Количество полей соответствует количеству узлов контроллера.

   - Если вы хотите изменить номер TCP-порта узла контроллера, в поле **Порт** введите номер базового порта. Диапазон значений: от 1 до 65 535. Значение по умолчанию: `6653`. Количество полей соответствует количеству узлов контроллера.

     Вместе с базовым портом узла контроллера автоматически указываются порты с тремя следующими по порядку номерами. Например, если вы вводите номер базового порта `6653`, автоматически указываются порты 6654, 6655 и 6656.

   - Если вы хотите указать узел-арбитр, установите флажок **Арбитр** рядом с узлом контроллера. Вы не можете указать узел-арбитр, если при развертывании экземпляра SD-WAN вы развернули один узел контроллера.

4. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры экземпляра SD-WAN.

Просмотр использования экземпляра SD-WAN

При необходимости вы можете посмотреть, какие устройства CPE были добавлены для экземпляра SD-WAN.

Чтобы посмотреть, используется ли экземпляр SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN, использование которого вы хотите посмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Конфигурация**, на которой отображается основная информация об экземпляре SD-WAN.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Показать связанные CPE**.

Откроется раздел **CPE**, в котором отображается таблица устройств CPE, добавленных экземпляру SD-WAN.

Просмотр топологии экземпляра SD-WAN

Чтобы посмотреть топологию экземпляра SD-WAN:

1. Войдите на портал самообслуживания тенанта, для которого развернут экземпляр SD-WAN.

2. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

3. Нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

4. Перейдите в раздел **Топология**.

   Отобразится топология экземпляра SD-WAN.

5. При необходимости установите следующие флажки:

   - Установите флажок **Использование соединения**, чтобы отобразить загруженность соединений. Уровень загруженности соединения соответствует следующим цветам:

     - Зеленый – малая загруженность соединения.
     - Желтый – средняя загруженность соединения.
     - Красный – высокая загруженность соединения.

   - Установите флажок **Сегменты** и в раскрывающемся списке **Коммутаторы сегмента** выберите два устройства CPE, чтобы отобразить все соединения между этими устройствами CPE.
   - Установите флажок **Имя**, чтобы отобразить имена устройств CPE.
   - Установите флажок **IP-адрес**, чтобы отобразить IP-адреса устройств CPE.

   По умолчанию все флажки сняты.

Добавление тенанта в экземпляр SD-WAN

Если вы хотите использовать контроллер одного экземпляра SD-WAN для нескольких тенантов, вам нужно добавить тенантов в экземпляр SD-WAN. Использование контроллера одного экземпляра SD-WAN для нескольких тенантов позволяет не развертывать отдельный экземпляр SD-WAN для каждого тенанта.

Чтобы добавить тенанта в экземпляр SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN, в который вы хотите добавить тенанта.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию выбрана вкладка **Конфигурация**, на которой отображается основная информация об экземпляре SD-WAN.

3. Выберите вкладку **Самообслуживание тенанта**.

   Отобразится таблица тенантов.

4. Нажмите на кнопку **+ Добавить**.

5. В открывшемся окне выберите созданного тенанта, которого вы хотите добавить в экземпляр SD-WAN.

6. В поле **Максимум CPE** введите максимальное количество доступных тенанту устройств CPE.

7. Нажмите на кнопку **Добавить**.

Тенант будет добавлен в экземпляр SD-WAN и отобразится в таблице.

Удаление тенанта из экземпляра SD-WAN

Вы можете удалить тенанта, который был добавлен в экземпляр SD-WAN, чтобы тенант не использовал контроллер экземпляра SD-WAN.

Чтобы удалить тенанта из экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN, из которого вы хотите удалить тенанта.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Конфигурация**, на которой отображается основная информация об экземпляре SD-WAN.

3. Выберите вкладку **Самообслуживание тенанта**.

   Отобразится таблица тенантов.

4. Нажмите на кнопку **Удалить** рядом с тенантом, которого вы хотите удалить из экземпляра SD-WAN.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Тенант будет удален из экземпляра SD-WAN и перестанет отображаться в таблице.

Удаление экземпляра SD-WAN

При удалении экземпляра SD-WAN автоматически удаляются добавленные ему устройства CPE и сетевой сервис SD-WAN, развернутый в экземпляре SD-WAN. При этом тенант, для которого был развернут экземпляр SD-WAN, не удаляется. Альтернативным способом удаления экземпляра SD-WAN является удаление сетевого сервиса SD-WAN.

Удаленные экземпляры SD-WAN невозможно восстановить.

Чтобы удалить экземпляр SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN, который вы хотите удалить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Конфигурация**, на которой отображается основная информация об экземпляре SD-WAN.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Экземпляр SD-WAN будет удален и перестанет отображаться в таблице.

Работа с пулами экземпляров SD-WAN

Вы можете посмотреть таблицу пулов экземпляров SD-WAN в разделе **SD-WAN → Пулы экземпляров SD-WAN**. Информация о пулах экземпляров SD-WAN отображается в следующих столбцах таблицы:

- **ID** – идентификатор пула экземпляров SD-WAN.
- **Имя** – имя пула экземпляров SD-WAN.
- **Количество экземпляров** – количество экземпляров SD-WAN в пуле экземпляров SD-WAN.
- **[[sdwan.cpeCount]]** – количество устройств CPE, которые были добавлены экземплярам SD-WAN.
- **Создан** – дата и время создания пула экземпляров SD-WAN.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Параметры пула экземпляров SD-WAN можно настроить на следующих вкладках:

- **Информация** – основная информация о пуле экземпляров SD-WAN. Вы можете изменить имя пула экземпляров SD-WAN в поле **Имя** и ввести его краткое описание в поле **Описание**.
- **Экземпляры SD-WAN** – экземпляры SD-WAN, которые были добавлены в пул экземпляров SD-WAN.

Создание пула экземпляров SD-WAN

Чтобы создать пул экземпляров SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Пулы экземпляров SD-WAN**.

   Отобразится таблица пулов экземпляров SD-WAN.

2. В верхней части страницы нажмите на кнопку **+ Пул экземпляров SD-WAN**.
3. В открывшемся окне введите имя пула экземпляров SD-WAN.
4. Нажмите на кнопку **Создать**.

Пул экземпляров SD-WAN будет создан и отобразится в таблице.

Вам нужно добавить экземпляры SD-WAN в созданный пул экземпляров SD-WAN.

Добавление экземпляра SD-WAN в пул экземпляров SD-WAN

Чтобы добавить экземпляр SD-WAN в пул экземпляров SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Пулы экземпляров SD-WAN**.

   Отобразится таблица пулов экземпляров SD-WAN.

2. Нажмите на пул экземпляров SD-WAN, в который вы хотите добавить экземпляр SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о пуле экземпляров SD-WAN.

3. Выберите вкладку **Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

4. Нажмите на кнопку **+ Добавить**.

5. В открывшемся окне выберите развернутый экземпляр SD-WAN, который вы хотите добавить в пул экземпляров SD-WAN.

6. Нажмите на кнопку **Добавить**.

   Экземпляр SD-WAN будет добавлен в пул экземпляров SD-WAN и отобразится в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры пула экземпляров SD-WAN.

Если вы добавляете устройство CPE в пул экземпляров SD-WAN, устройство CPE может быть добавлено экземпляру SD-WAN, который вы добавили в пул экземпляров SD-WAN. Это происходит, если экземпляру SD-WAN добавлено наименьшее количество устройств CPE по сравнению с другими экземплярами SD-WAN в пуле экземпляров SD-WAN.

Удаление экземпляра SD-WAN из пула экземпляров SD-WAN

Чтобы удалить экземпляр SD-WAN из пула экземпляров SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Пулы экземпляров SD-WAN**.

   Отобразится таблица пулов экземпляров SD-WAN.

2. Нажмите на пул экземпляров SD-WAN, из которого вы хотите удалить экземпляр SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о пуле экземпляров SD-WAN.

3. Выберите вкладку **Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

4. Нажмите на кнопку **Удалить** рядом с экземпляром SD-WAN, который вы хотите удалить из пула экземпляров SD-WAN.

   Экземпляр SD-WAN будет удален из пула экземпляров SD-WAN и перестанет отображаться в таблице.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры пула экземпляров SD-WAN.

Удаление пула экземпляров SD-WAN

Когда вы удаляете пул экземпляров SD-WAN, автоматически удаляются все устройства CPE, добавленные пулу экземпляров SD-WAN. Экземпляры SD-WAN при этом не удаляются.

Удаленные пулы экземпляров SD-WAN невозможно восстановить.

Чтобы удалить пул экземпляров SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Пулы экземпляров SD-WAN**.

   Отобразится таблица пулов экземпляров SD-WAN.

2. Нажмите на пул экземпляров SD-WAN, который вы хотите удалить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о пуле экземпляров SD-WAN.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Пул экземпляров SD-WAN будет удален и перестанет отображаться в таблице.

Управление устройствами CPE

Устройства CPE передают трафик между площадками вашей организации и клиентами, а также имеют прямой доступ в интернет (англ. Direct Internet Access, DIA) без перенаправления трафика в центральный офис. Для построения сети SD-WAN на устройствах CPE по умолчанию установлен виртуальный коммутатор OpenFlow (англ. OpenFlow virtual switch, далее также виртуальный коммутатор или vSwitch). Вы можете использовать устройства CPE следующих типов:

- Устройства CPE модели KESR (Kaspersky SD-WAN Edge Service Router), приобретенные у "Лаборатории Касперского".
- Виртуальные устройства CPE (далее также устройства vCPE), развернутые на виртуальных машинах. При использовании устройств vCPE вам нужно убедиться, что виртуальные машины соответствуют аппаратным и программным требованиям.
- Универсальные устройства CPE (далее также устройства uCPE), поддерживающие развертывание VIM и виртуальных сетевых функций.

Для управления устройствами CPE вам нужно их зарегистрировать.

Вы можете использовать *двухфакторную аутентификацию*, чтобы безопасно зарегистрировать устройство CPE. При включенной двухфакторной аутентификации в базу данных оркестратора записывается токен (ключ безопасности), который затем вы помещаете на устройство CPE при регистрации с использованием технологии Zero Touch Provisioning. Регистрация проходит успешно, если при автоматическом подключении устройства CPE к оркестратору помещенный на устройство CPE токен совпадает с токеном в базе данных оркестратора.

Для централизованной настройки устройств CPE используются шаблоны CPE. Вам нужно указать параметры в шаблоне CPE, после чего указать шаблон CPE при добавлении или ручной регистрации устройств CPE, чтобы не настраивать каждое отдельное устройство CPE. Если вы измените параметр в шаблоне CPE, параметр автоматически изменится на всех устройствах CPE, которые используют шаблон CPE. Если вы измените параметр на устройстве CPE, параметр перестанет зависеть от шаблона CPE и при изменении в шаблоне CPE не будет изменяться на устройстве CPE.

> Определенные параметры устройства CPE можно указать только в шаблоне CPE, например номер порта для подключения к оркестратору.

Когда вы удаляете устройство CPE из веб-интерфейса оркестратора, на устройстве CPE сохраняются базовые параметры. Вы можете повторно зарегистрировать устройство CPE. При повторной регистрации устройства CPE невозможно использовать двухфакторную аутентификацию.

При добавлении и регистрации устройства CPE вы можете выбрать, должно ли устройство CPE автоматически включиться (англ. enable) после регистрации. Когда устройство CPE включено, к нему применяется шаблон CPE, и устройство CPE становится доступным для передачи трафика.

Вы можете сбросить параметры устройства CPE до заводских значений, не удаляя его из оркестратора, с помощью расположенной на устройстве физической кнопки Reset. Для этого необходимо нажать и удерживать кнопку в течение 10 секунд. Данный функционал доступен для моделей KESR M1,M2 и M3.

О взаимодействии между устройством CPE и оркестратором

После регистрации устройство CPE отправляет REST API-запросы оркестратору для получения задач с периодичностью, указанной при настройке подключения устройства CPE к оркестратору и контроллеру. *Задачи* – это действия, которые пользователи выполняют с устройством CPE, например перезагрузка устройства CPE и обновление прошивки. REST API-запросы необходимы для получения, задач, которые не связаны с виртуальным коммутатором устройства CPE.

Для просмотра таблицы выполняемых оркестратором задач на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE** и нажать на устройство CPE. Информация о задачах отображается в следующих столбцах таблицы:

- **Тип** – тип задачи.
- **Статус** – статус задачи:
  - **Ожидание** – задача помещена в базу данных оркестратора и ожидает получения устройством CPE.
  - **Выполнение** – задача выполняется.
  - **Завершено** – задача успешно выполнена.
  - **Ошибка** – при выполнении задачи произошла ошибка.
- **Последнее обновление** – дата и время последнего обновления задачи.

Выполнение оркестратором задач на устройстве CPE происходит следующим образом:

1. Вы выполняете задачу на устройстве CPE в веб-интерфейсе оркестратора, например изменяете параметры протокола BGP.
2. Оркестратор сохраняет задачу в базе данных. В таблице задача отображается со статусом **Ожидание**.
3. Устройство CPE получает задачу при отправлении REST API-запроса оркестратору. В таблице задача отображается со статусом **Выполнение**.
4. При успешном выполнении задачи устройство CPE сообщает об этом оркестратору. В таблице задача отображается со статусом **Завершено**.

   При невозможности выполнения задачи в таблице она отображается со статусом **Ошибка**.

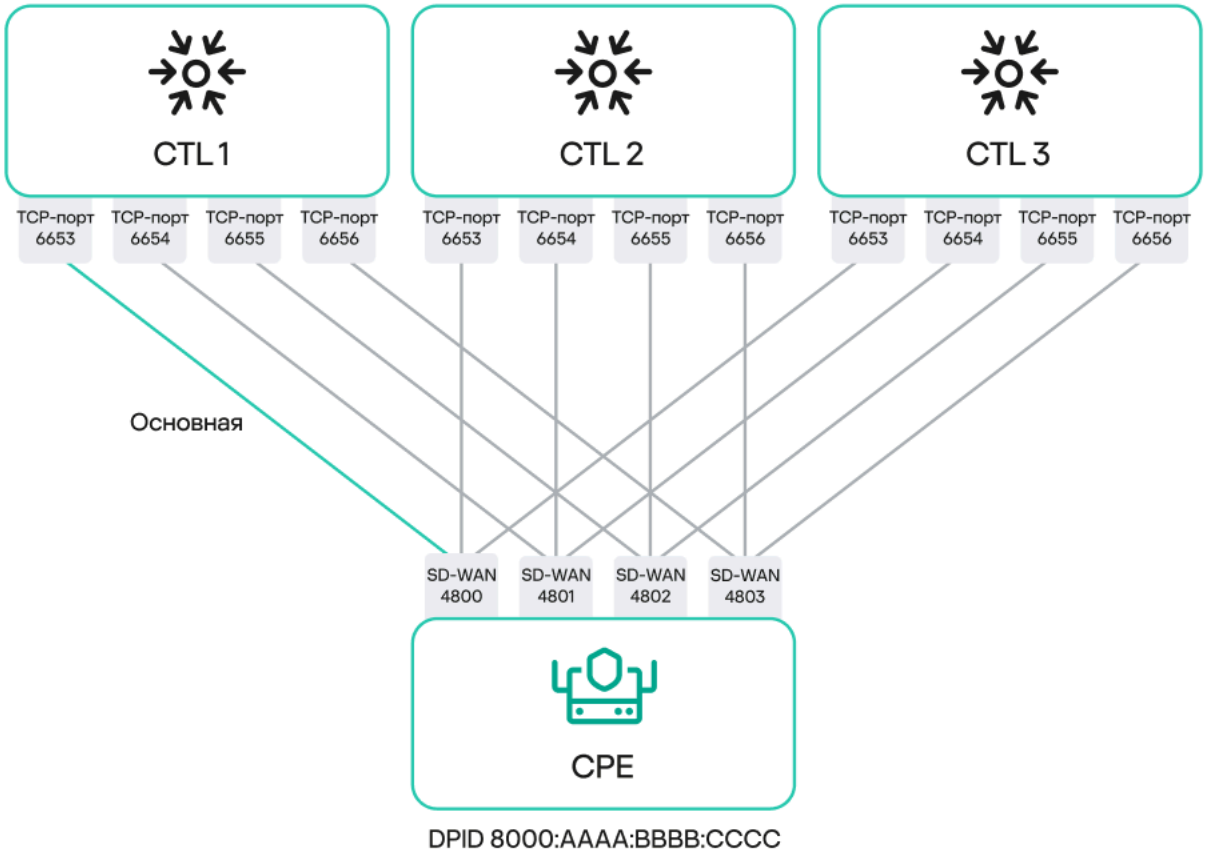
Перед выполнением задачи на устройстве CPE сохраняются текущие параметры. Если после успешного выполнения задачи устройство CPE не может отправить оркестратору сообщение с подтверждением, после трех попыток на устройстве CPE указываются предыдущие параметры, а в таблице задача отображается со статусом в **Ошибка**.

О взаимодействии между устройством CPE и контроллером

После регистрации устройства CPE между его интерфейсами SD-WAN с типом WAN и TCP-портами узлов контроллера устанавливаются *управляющие сессии*. Одна из управляющих сессий является основной (англ. primary session), а остальные находятся в режиме ожидания. По основной управляющей сессии передаются задачи, связанные с управлением виртуальным коммутатором устройства CPE, например изменение параметров путей. Если основная управляющая сессия разрывается, новая основная управляющая сессия выбирается случайно из ранее установленных управляющих сессий.

Управляющие сессии устанавливаются на основании порядкового соответствия номеров OpenFlow-портов, на которые ссылаются интерфейсы SD-WAN с типом WAN, и номеров TCP-портов узлов контроллера. Например, на рисунке ниже устройство CPE имеет четыре интерфейса SD-WAN, которые ссылаются на OpenFlow-порты с номерами 4800 ,4801, 4802 и 4803. Узлы контроллера CTL 1–3 имеют TCP-порты с номерами 6653, 6654, 6655, 6656. В этом случае управляющие сессии устанавливаются следующим образом:

- SD-WAN 4800 → 6653;
- SD-WAN 4801 → 6654;
- SD-WAN 4802 → 6655;
- SD-WAN 4803 → 6656.



Управляющие сессии между устройством CPE и тремя узлами контроллера

Параметры управляющих сессий можно указать при настройке подключения устройства CPE к оркестратору и контроллеру. Например, вы можете выбрать, с какого интерфейса SD-WAN с типом WAN в приоритете устанавливается основная управляющая сессия, а также указать, шифруются ли управляющие сессии.

Вы можете изменить IP-адреса и номера TCP-портов узлов контроллера при настройке узлов контроллера экземпляра SD-WAN. В этом случае IP-адреса и номера TCP-портов узлов контроллера автоматически изменятся на всех устройствах CPE, которые добавлены экземпляру SD-WAN. Если интерфейсы SD-WAN с типом WAN устройства CPE подключены к разным сетям, например к интернету и частной MPLS-сети, вы можете изменить IP-адреса и номера TCP-портов узлов контроллера на отдельных интерфейсах SD-WAN с типом WAN при создании или изменении интерфейсов SD-WAN с типом WAN. IP-адреса и номера TCP-портов, указанные на отдельном интерфейсе SD-WAN с типом WAN, являются более приоритетными по отношению к IP-адресам и номерам TCP-портов, указанным при настройке узлов контроллера экземпляра SD-WAN.

Для просмотра таблицы устройств CPE с информацией об управляющих сессиях вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **Коммутаторы**. Информация об управляющих сессиях отображается в следующих столбцах таблицы:

- **Имя** – имя устройства CPE.
- **Порядок** – порядковый номер устройства CPE. Наименьший порядковый номер присваивается устройству CPE, которое первым подключилось к контроллеру.
- **Статус** – статус устройства CPE по отношению к контроллеру:
  - **Активный** – устройство CPE можно использовать для передачи трафика.
  - **Неактивный** –устройство CPE невозможно использовать для передачи трафика.
- **Подключение** – статус подключения устройства CPE к контроллеру:
  - **Подключен** – между устройством CPE и узлами контроллера установлены управляющие сессии.
  - **Отключен** – между устройством CPE и узлами контроллера не установлены управляющие сессии.
- **MAC** – MAC-адрес устройства CPE.
- **Интерфейс** – интерфейсы SD-WAN с типом WAN, с которых установлены управляющие сессии.
- **Основная сессия** – интерфейс SD-WAN с типом WAN, с которого установлена основная управляющая сессия:
  - **Да**.
  - **Нет**.
- **IP** – IP-адрес, с помощью которого интерфейс SD-WAN с типом WAN установил управляющую сессию.
- **Порт** – номер TCP-порта, с помощью которого интерфейс SD-WAN с типом WAN установил управляющую сессию.
- **Создан** – дата и время регистрации устройства CPE.
- **Расположение** – адрес площадки устройства CPE.

- **Задержка (мс)** – время задержки в миллисекундах для управляющей сессии.
- **Описание** – краткое описание устройства CPE.

Учетные данные по умолчанию устройств CPE модели KESR

Все устройства CPE модели KESR (Kaspersky SD-WAN Edge Service Router) имеют одинаковые учетные данные по умолчанию:

- Имя учетной записи: `root`
- Пароль: `123-qwe`

Вам потребуется ввести эти учетные данные, чтобы подключиться к незарегистрированному устройству CPE модели KESR по протоколу SSH или установить с ним консольную сессию. После регистрации пароль по умолчанию устройства CPE автоматически изменится. Вы можете посмотреть пароль устройства CPE в веб-интерфейсе оркестратора.

Проверка целостности

Эта функция позволяет автоматически или вручную проверять целостность критически важных файлов, отвечающих за работу системы и firewall в частности, сравнивая их с эталонными контрольными суммами. Она может обнаруживать несанкционированные изменения и гарантирует, что системные сценарии и исполняемые файлы соответствуют выпущенной прошивке.

Вы можете запускать проверку по требованию или настроить проверку по расписанию.

Проверку по требованию можно запускать только на устройстве CPE.

Для этого перейдите в меню оркестратора **Шаблоны CPE**, выберите шаблон, далее перейдите в пункт меню SD-WAN → вкладка «Проверки CPE» и нажмите кнопку «Запустить» раздела «Проверка целостности» в секции «Ручная проверка».

На CPE стартует утилита, которая проводит проверку и выводит информацию в системный журнал CPE.

При этом в разделе «Проверка целостности» секции «Ручная проверка» отмечается, что задача запущена и фиксируется дата и время запуска. Здесь же отображается статус выполнения.

Также оркестратор отображает статус и результат проверки в пользовательском интерфейсе на устройстве CPE в меню «Главное», в секции «Внеполосное управление». После запуска задача «Проверка целостности» имеет статус «Выполнение». Далее, в зависимости от результатов работы утилиты, CPE передает оркестратору статус «Успешно» или «Ошибка». ????

Проверка по расписанию может настраиваться как в шаблоне CPE, так и самом устройстве CPE.

Для настройки перейдите в меню оркестратора Шаблоны CPE, выберите шаблон, далее перейдите в пункт меню SD-WAN → вкладка «Проверки CPE» и нажмите на переключатель «Проверка целостности» в секции «Расписание проверок».

На CPE нужно будет предварительно нажать на переключатель «Переопределить» .

Теперь можно установить интервал между проверками.

На CPE будет запускаться утилита, которая проводит проверку и выводит информацию в системный журнал CPE.

Оркестратор отображает статус и результат проверки в пользовательском интерфейсе на устройстве CPE в меню «Главное», в секции «Внеполосное управление». ????

Дополнительно можно заблокировать передачу трафика при неудачных проверках.

Регистрация устройств CPE

Существуют следующие сценарии регистрации устройств CPE:

- Регистрация устройства CPE с использованием технологии Zero Touch Provisioning (ZTP). Этот сценарий применим к новым устройствам CPE, которые ранее не были зарегистрированы.
- Развертывание на платформе виртуализации VMware и регистрация устройства vCPE с использованием технологии Zero Touch Provisioning. Этот сценарий применим к виртуальным устройствам CPE, которые развертываются на виртуальных машинах.
- Повторная регистрация устройства CPE. Этот сценарий применим к ранее зарегистрированным устройствам CPE, которые были удалены.

Во время регистрации устройства CPE не требуется подключаться к серверам активации лицензий и обновлений "Лаборатории Касперского", а также к серверам KSN (Kaspersky Security Network). Если при регистрации устройства CPE возникает ошибка, вы можете возобновить регистрацию устройства CPE.

Сценарий: регистрация устройства CPE с использованием технологии Zero Touch Provisioning

Вы можете зарегистрировать новые устройства CPE, используя технологию Zero Touch Provisioning (далее также ZTP). Технология ZTP позволяет устройству CPE автоматически подключится к оркестратору.

При использовании технологии ZTP требуется сгенерировать веб-адрес с базовыми параметрами устройства CPE. *Базовыми параметрами* являются параметры, которые необходимы для автоматического подключения устройства CPE к оркестратору. Для завершения регистрации вам нужно подключить к устройству CPE устройство администратора и перейти на устройстве администратора по сгенерированному веб-адресу с базовыми параметрами.

Сценарий регистрации устройства CPE с использованием технологии ZTP состоит из следующих этапов:

1. **Создание шаблона CPE**

   Создайте и настройте шаблон CPE. Более подробно о работе с шаблонами CPE см. в разделе Работа с шаблонами CPE. Вы можете использовать созданный шаблон CPE для настройки других устройств CPE.

2. **Добавление устройства CPE**

Добавьте устройство CPE. При добавлении устройства CPE укажите созданный шаблон CPE и выберите, должно ли устройство CPE автоматически включиться после регистрации. Добавленное устройство CPE имеет статус **Ожидание**. Более подробно о работе с устройствами CPE см. в разделе Работа с устройствами CPE.

3. **Двухфакторная аутентификация (необязательный этап)**

   Если вы хотите безопасно зарегистрировать устройство CPE, используйте двухфакторную аутентификацию.

4. **Генерация веб-адреса с базовыми параметрами**

   Сгенерируйте веб-адрес с базовыми параметрами устройства CPE.

5. **Регистрация устройства CPE**

   Выполните следующие действия:

   1. Подключите устройство администратора к LAN-порту устройства CPE.

      Устройство администратора получит IP-адрес и IP-адрес шлюза по умолчанию по протоколу DHCP. Полученный IP-адрес шлюза по умолчанию является IP-адресом устройства CPE.

   2. Перейдите по сгенерированному веб-адресу с базовыми параметрами устройства CPE на устройстве администратора одним из следующих способов:

      - В адресной строке браузера введите веб-адрес с базовыми параметрами устройства CPE и нажмите на клавишу **Enter**.
      - Откройте файл HTML-файл, который вы сохранили при генерации веб-адреса с базовыми параметрами устройства CPE.

   3. На открывшейся странице нажмите на кнопку **Применить конфигурацию**.

   Устройство CPE автоматически подключится к оркестратору, привяжется к добавленному устройству CPE в веб-интерфейсе оркестратора и зарегистрируется. Зарегистрированное устройство CPE имеет статус **Зарегистрировано** и находится в состоянии **Включено** или **Выключено**.

6. **Включение устройства CPE (необязательный этап)**

   Если при добавлении устройства CPE вы указали, что оно не должно автоматически включиться, включите устройство CPE. Включенное устройство CPE имеет статус **Зарегистрировано** и находится в состоянии **Включено**.

7. **Включение шифрования трафика на устройстве (необязательный этап)**

   Если необходимо использовать шифрование трафика на устройстве CPE, включите его для всего устройства или для отдельного соединения.

Сценарий: развертывание на платформе виртуализации VMware и регистрация устройства vCPE с использованием технологии Zero Touch Provisioning

Вы можете развернуть устройство vCPE на платформе виртуализации VMware с помощью шаблона OVF, после чего зарегистрировать устройство vCPE, используя технологию ZTP.

Шаблон OVF – это архив knaas-cpe_<версия прошивки>.release.<номер версии решения>.combined.adm64-legacy.vKESR-M1-esxi.tar.gz, который содержится в директории /cpe комплекта поставки и содержит следующие файлы:

- vKESR.mf – хеш-сумма SHA256 файлов шаблона OVF.
- vKESR.nvram – состояние BIOS виртуальной машины.
- vKESR.ovf – дескриптор, содержащий информацию о параметрах виртуальной машины.
- vKESR.vmdk – образ диска виртуальной машины.

Вам нужно скачать шаблон OVF и распаковать его на локальном устройстве перед выполнением этого сценария.

Сценарий развертывания на платформе виртуализации VMware и регистрации устройства vCPE с использованием технологии ZTP состоит из следующих этапов:

1. **Создание шаблона vCPE**

   Создайте и настройте шаблон vCPE. Более подробно о работе с шаблонами vCPE см. в разделе Работа с шаблонами CPE. Вы можете использовать созданный шаблон vCPE для настройки других устройств vCPE.

2. **Добавление устройства vCPE**

   Добавьте устройство vCPE. При добавлении устройства vCPE выполните следующие действия:

   - укажите созданный шаблон vCPE;
   - выберите, должно ли устройство vCPE автоматически включиться после регистрации;
   - укажите временный идентификатор DPID устройства vCPE, например `temporary DPID`.

   Добавленное устройство vCPE имеет статус **Ожидание**. Более подробно о работе с устройствами vCPE см. в разделе Работа с устройствами CPE.

3. **Двухфакторная аутентификация (необязательный этап)**

   Если вы хотите безопасно зарегистрировать устройство vCPE, используйте двухфакторную аутентификацию.

4. **Генерация веб-адреса с базовыми параметрами**

   Сгенерируйте веб-адрес с базовыми параметрами устройства vCPE.

5. **Развертывание устройства vCPE на платформе виртуализации VMware**

   В веб-интерфейсе платформы виртуализации VMware создайте виртуальную машину для развертывания устройства vCPE. Убедитесь, что создаваемая виртуальная машина соответствует аппаратным и программным требованиям. При создании виртуальной машины выполните следующие действия:

   1. Выберите способ создания виртуальной машины с использованием стандарта OVF или файла OVA.
   2. При выборе файлов VDMK укажите файлы распакованного на локальном устройстве шаблона OVF.
   3. При настройке дополнительных параметров укажите сгенерированный веб-адрес с базовыми параметрами.

   Более подробную информацию о создании виртуальных машин можно получить из официальной документации VMware.

При успешном применении параметров устройство vCPE автоматически подключится к оркестратору и отобразится в веб-интерфейсе оркестратора со статусом **Неизвестно**.

6. **Регистрация устройства vCPE**

   Измените временный идентификатор DPID, который вы указали при добавлении устройства vCPE, на настоящий идентификатор DPID устройства vCPE. Настоящим идентификатором DPID устройства vCPE является имя хоста виртуальной машины, на которой развернуто устройство vCPE. Имя хоста виртуальной машины отображается в веб-интерфейсе платформы виртуализации VMware.

   Устройство vCPE привяжется к добавленному устройству vCPE в веб-интерфейсе оркестратора и зарегистрируется. Зарегистрированное устройство vCPE имеет статус **Зарегистрировано** и находится в состоянии **Включено** или **Выключено**.

7. **Включение устройства vCPE (необязательный этап)**

   Если при добавлении устройства vCPE вы указали, что оно не должно автоматически включиться, включите устройство vCPE. Включенное устройство vCPE имеет статус **Зарегистрировано** и находится в состоянии **Включено**.

Сценарий: повторная регистрация устройства CPE

Если вы удаляете устройство CPE, на нем сохраняются базовые параметры. Вы можете повторно зарегистрировать удаленное устройство CPE без использования технологии ZTP.

> При повторной регистрации устройства CPE невозможно использовать двухфакторную аутентификацию. Если вы хотите использовать двухфакторную аутентификацию, зарегистрируйте устройство CPE с использованием технологии ZTP.

Сценарий повторной регистрации устройства CPE состоит из следующих этапов:

1. **Перевод прошивки устройства CPE в стартовое состояние**

   Подключитесь к устройству CPE по протоколу SSH. Для этого укажите IP-адрес и введите учетные данные устройства CPE. Затем выполните команду:

   ```
   firstboot && reboot
   ```

2. **Создание шаблона CPE**

   Создайте и настройте шаблон CPE. Подробнее о работе с шаблонами CPE см. в разделе Работа с шаблонами CPE. Вы можете использовать созданный шаблон CPE для настройки других устройств CPE.

3. **Подключение устройства CPE к оркестратору**

   Отключите и подключите кабель питания устройства CPE, чтобы оно перезагрузилось и подключилось к оркестратору. При успешном подключении устройство CPE отобразится в веб-интерфейсе оркестратора со статусом **Неизвестно**.

4. **Ручная регистрация устройства CPE**

   Вручную зарегистрируйте устройство CPE. При ручной регистрации устройства CPE укажите созданный шаблон CPE и выберите, должно ли устройство CPE автоматически включиться после регистрации. Зарегистрированное устройство имеет статус **Зарегистрировано** и находится в состоянии **Включено** или **Выключено**. Подробнее о работе с устройствами CPE см. в разделе Работа с устройствами CPE.

5. **Включение устройства CPE (необязательный этап)**

Если при ручной регистрации устройства CPE вы указали, что оно не должно автоматически включиться, включите устройство CPE. Включенное устройство CPE имеет статус **Зарегистрировано** и находится в состоянии **Включено**.

Возобновление регистрации устройства CPE при возникновении ошибки

Если при регистрации устройства CPE возникает ошибка, статус устройства CPE изменяется на **Приостановлен** и регистрация не завершается.

Чтобы возобновить регистрацию устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. В столбце **Статус** нажмите на статус устройства CPE.

   Откроется журнал выполнения сервисного запроса.

3. Нажмите на шаг, на котором произошла ошибка, чтобы посмотреть информацию о возможных причинах возникновения ошибки, а также о действиях по исправлению ошибки.

4. Если вы хотите отменить регистрацию устройства CPE, нажмите на кнопку **Отмена**.

5. После выполнения действий по исправлению ошибки нажмите на кнопку **Продолжить**, чтобы возобновить регистрацию устройства CPE. В некоторых случаях после возобновления регистрации устройство CPE необходимо перезагрузить.

Регистрация устройства CPE будет возобновлена.

Если вам не удается зарегистрировать устройство CPE, мы рекомендуем обратиться в техническую поддержку "Лаборатории Касперского".

Работа с шаблонами CPE

Вы можете посмотреть таблицу шаблонов CPE в разделе **SD-WAN → Шаблоны CPE**. Информация о шаблонах CPE отображается в следующих столбцах таблицы:

- **ID** – идентификатор шаблона CPE.
- **Имя** – имя шаблона CPE.
- **Использование** – использование шаблона CPE устройствами CPE:
  - **Да**.
  - **Нет**.
- **Изменено** – дата и время последнего изменения параметров шаблона CPE.

- **Пользователь** – имя пользователя, который создал шаблон CPE.
- **Владелец** – тенант, к которому относится шаблон CPE.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Параметры шаблона CPE можно настроить на следующих вкладках:

- **Информация** – основная информация о шаблоне CPE. Вы можете изменить имя шаблона CPE в поле **Имя**.
- **Мультипутевая передача** – параметры путей.
- **Деактивация** – параметры автоматического удаления и выключения устройства CPE.
- **Шифрование** – параметры шифрования трафика.
- **Скрипты** – скрипты для дополнительной настройки устройства CPE.
- **SD-WAN** – параметры подключения устройства CPE к сети SD-WAN. На этой вкладке отображаются следующие вкладки:
  - **Основные параметры** – параметры подключения устройства CPE к оркестратору и контроллеру.
  - **Интерфейсы** – интерфейсы SD-WAN.
- **Топология** – топологические теги для построения соединений между устройствами CPE.
- **Сеть** – сетевые интерфейсы.
- **BGP** – настройки параметров использования протокола BGP для обмена маршрутами между устройствами CPE и внешними сетевыми устройствами.
- **VRF** – виртуальные таблицы маршрутизации.
- **OSPF** – протокол OSPF для обмена маршрутами между устройствами CPE и внешними сетевыми устройствами. На этой вкладке отображаются следующие вкладки:
  - **Основные параметры** – основные параметры протокола OSPF.
  - **OSPF-области** – OSPF-области.
  - **OSPF-интерфейсы** – OSPF-интерфейсы.
- **Фильтры маршрутов** – параметры фильтрации маршрутов и пакетов трафика между устройствами CPE и внешними сетевыми устройствами. На этой вкладке отображаются следующие вкладки:
  - **Списки управления доступом** – списки управления доступом (ACLs).
  - **Списки префиксов** – списки префиксов (prefix lists).
  - **Карты маршрутизации** – карты маршрутизации (route maps).
- **BFD** – протокол BFD для обнаружения ошибок маршрутизации между устройствами CPE и внешними сетевыми устройствами.

- **Статические маршруты** – статические маршруты.
- **Multicast** – параметры передачи multicast-трафика между устройствами CPE и внешними сетевыми устройствами с помощью протоколов PIM и IGMP. На этой вкладке отображаются следующие вкладки:
  - **Основные параметры** – основные параметры PIM.
  - **Интерфейсы** – multicast-интерфейсы.
- **VRRP** – протокол VRRP для обеспечения высокой доступности устройств CPE. На этой вкладке отображаются следующие вкладки:
  - **Экземпляры VRRP** – экземпляры VRRP.
  - **Группы экземпляров VRRP** – группы экземпляров VRRP.
- **CFM** – параметры функции Connectivity Fault Management (CFM).
- **Мониторинг** – параметры мониторинга устройства CPE.
- **Транспортные сервисы** – транспортные сервисы.
- **Запись в журнал** – параметры журналов.
- **NTP** – NTP-серверы для синхронизации времени.
- **VIM** – параметры VIM. Эта вкладка отображается, только если при создании шаблона CPE вы выбрали тип **uCPE**.

Создание шаблона CPE

Чтобы создать шаблон CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. В верхней части страницы нажмите на кнопку **+ Шаблон CPE**.

3. В открывшемся окне в поле **Имя** введите имя шаблона CPE.

4. В раскрывающемся списке **Тип** выберите тип шаблона CPE:
   - **CPE** – шаблон стандартного устройства CPE. Это значение выбрано по умолчанию.
   - **uCPE** – шаблон устройства uCPE. В состав устройства uCPE входит гипервизор, поэтому на устройстве uCPE можно развернуть виртуальные сетевые функции и VIM.

5. Нажмите на кнопку **Создать**.

Шаблон CPE будет создан и отобразится в таблице.

Вам нужно настроить созданный шаблон CPE. Более подробно о работе с шаблонами CPE см. в разделе Работа с шаблонами CPE.

Импорт шаблона CPE

Вы можете экспортировать шаблон CPE, после чего импортировать его в другой шаблон CPE. Параметры шаблона CPE выстраиваются в соответствии с параметрами импортированного шаблона CPE. При импорте можно выбрать вкладки, которые вы хотите оставить без изменений.

Чтобы импортировать шаблон CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, который вы хотите экспортировать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Экспортировать**.

   На ваше локальное устройство сохранится архив в формате TAR.GZ со следующими данными:

   - Файл с описанием шаблона CPE в формате XML. В описании указывается версия шаблона.
   - Файлы скриптов.
   - Файлы для запуска скриптов, например SSL-сертификаты.

   В архиве не содержится информация об устройствах CPE, использующих шаблон CPE.

4. Нажмите на шаблон CPE, в который вы хотите импортировать шаблон CPE.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

5. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Импортировать**.

6. В открывшемся окне снимите флажки рядом со вкладками шаблона CPE, которые вы хотите оставить без изменения после импорта.

7. В поле **Файл** укажите путь к архиву в формате TAR.GZ.

8. Нажмите на кнопку **Импортировать**.

Параметры шаблона CPE будут изменены в соответствии с параметрами импортированного шаблона CPE.

Клонирование шаблона CPE

Вы можете клонировать шаблон CPE, чтобы создать такой же шаблон CPE с другим именем.

Чтобы клонировать шаблон CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, который вы хотите клонировать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Клонировать**.

4. В открывшемся окне введите имя нового шаблона CPE.

5. Нажмите на кнопку **Клонировать**.

Клон шаблона CPE с новым именем будет создан и отобразится в таблице.

Экспорт параметров подключения к оркестратору и контроллеру, и интерфейсов SD-WAN из шаблона CPE

Чтобы экспортировать параметры подключения к оркестратору и контроллеру и интерфейсы SD-WAN из шаблона CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, из которого вы хотите экспортировать параметры подключения к оркестратору и контроллеру и интерфейсы SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Экспортировать параметры SD-WAN**.

На ваше локальное устройство сохранится файл в формате JSON с именем <Имя шаблона>sdwan-config.

Экспорт сетевых интерфейсов из шаблона CPE

Чтобы экспортировать сетевые интерфейсы из шаблона CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, из которого вы хотите экспортировать сетевые интерфейсы.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Экспортировать сетевые интерфейсы**.

На ваше локальное устройство сохранится файл в формате JSON с именем <Имя шаблона>-network-config.

Просмотр использования шаблона CPE

При необходимости вы можете посмотреть, какие устройства CPE используют шаблон CPE. Например, если шаблон CPE используется, его невозможно удалить.

Чтобы посмотреть, используется ли шаблон CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, использование которого вы хотите посмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Показать связанные CPE**.

Откроется раздел **CPE**, в котором отображается таблица устройств CPE, использующих шаблон CPE.

Удаление шаблона CPE

Вы не можете удалить шаблон CPE, если он используется хотя бы одним устройством CPE. Для удаления шаблона CPE, который используется устройствами CPE, вам нужно сначала удалить устройства CPE. Вы можете посмотреть, какие устройства CPE используют шаблон CPE.

Удаленные шаблоны CPE невозможно восстановить.

Чтобы удалить шаблон CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, который вы хотите удалить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Шаблон CPE будет удален и перестанет отображаться в таблице.

Работа с устройствами CPE

Вы можете посмотреть таблицу устройств CPE в разделе **SD-WAN → CPE**.

В верхней части таблицы доступны фильтры для быстрой фильтрации таблицы с учетом статуса устройства, состояния подключения, состояния питания и периода времени.

Информация об устройствах CPE отображается в следующих столбцах таблицы:

- **DPID** – идентификатор DPID устройства CPE.
- **C/H** – серийный номер устройства CPE.
- **Модель** – модель устройства CPE.
- **Тип коммутатора** – тип программного коммутатора, на основе которого сделана прошивка устройства CPE (OVS или SWOS).
- **Версия ПО** – версия прошивки устройства CPE. Устаревшие прошивки подсвечиваются оранжевым цветом.
- **Имя** – имя устройства CPE.
- **Роль** – роль устройства CPE:
  - **CPE**.
  - **Шлюз**.

- **Статус** – статус устройства CPE:
  - **Неизвестно** – устройство CPE подключено к оркестратору, но не зарегистрировано.
  - **Ожидание** – устройство CPE добавлено в веб-интерфейс оркестратора, но не подключено к оркестратору.
  - **Регистрация** – выполняется регистрация устройства CPE.
  - **Ошибка** – при регистрации устройства CPE возникла ошибка.
  - **Зарегистрировано** – устройство CPE успешно зарегистрировано.
  - **Конфигурация** – на устройстве CPE выполняется запуск скриптов.
  - **Приостановлен** – при регистрации устройства CPE возникла ошибка и регистрация не была завершена.
- **Состояние** – состояние устройства CPE:
  - **Включено** – со стороны оркестратора к устройству CPE применен назначенный шаблон CPE. Со стороны контроллера устройство CPE можно использовать для передачи трафика.
  - **Выключено** (в статусе **Ожидание**) – со стороны оркестратора к устройству CPE не применен назначенный шаблон CPE. Со стороны контроллера устройство CPE невозможно использовать для передачи трафика.
  - **Выключено** (в статусе **Зарегистрировано**) – оркестратор не отвечает на REST API-запросы, поступающие от устройства CPE. Со стороны контроллера устройству CPE заблокирована передача трафика через соединения.
- **Подключение** – информация о том, подключено ли устройство CPE к контроллеру:
  - **Подключено**.
  - **Отключено**.
- **Топологические теги** – топологические теги, которые были назначены устройству CPE.
- **Фрагментация** – результат проверки фрагментации пакетов трафика на устройстве CPE:
  - **Не поддерживается** – на устройстве CPE невозможна передача фрагментированных пакетов.
  - **Неизвестно** – на устройстве CPE невозможно проверить фрагментацию пакетов.
  - **Поддерживается** – на устройстве CPE возможна передача фрагментированных пакетов.
- **Транспортный тенант** – транспортный тенант, для которого было добавлено устройство CPE. Устройство CPE подключается к контроллеру экземпляра SD-WAN, который был развернут для транспортного тенанта.
- **Клиентский тенант** – клиентский тенант, для которого было добавлено устройство CPE. Клиентский тенант может управлять устройством CPE на своем портале самообслуживания.
- **Шаблон CPE** – шаблон CPE, используемый устройством CPE.

- **Расположение** – адрес расположения устройства CPE.
- **Управляющий IP** – IP-адрес, который управляющая подсеть назначила устройству CPE.
- **Контроллеры** – IP-адреса и номера портов узлов контроллера, к которым подключено устройство CPE.
- **Шлюзы** – IP-адреса и номера портов шлюзов, к которым подключено устройство CPE.
- **Мобильная сеть** – мобильная сеть, к которой подключено устройство CPE.
- **Зарегистрировано** – дата и время регистрации устройства CPE.
- **Обновлено** – дата и время последнего изменения параметров устройства CPE.
- **Пользователь** – имя пользователя, который добавил устройство CPE.
- **Статус питания** – статус питания устройства CPE:
  - **OK**
  - **Отказ БП**
  - **Аккумулятор**
  - **Неизвестно**

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Вы можете просматривать и настраивать параметры устройства CPE, нажав на его название в таблице и выбрав нужный раздел боковой панели в открывшемся окне:

- **Конфигурация** – основная информация об устройстве CPE. Информацию можно посмотреть в следующих столбцах таблицы **Информация об устройстве**:
  - **Модель** – модель устройства CPE.
  - **Версия ПО** – версия прошивки устройства CPE. Устаревшие прошивки подсвечиваются оранжевым цветом.
  - **Контроллер** – IP-адреса и номера портов узлов контроллера, к которым подключено устройство CPE.
  - **Шлюзы** – IP-адреса и номера портов шлюзов, к которым подключено устройство CPE.
  - **Пользователь** – имя пользователя, который добавил устройство CPE.
  - **Зарегистрировано** – дата и время регистрации устройства CPE.
  - **Обновлено** – дата и время последнего изменения параметров устройства CPE.
  - **Управляющий IP** – IP-адрес, который управляющая подсеть назначила устройству CPE.
  - **Состояние** – состояние устройства CPE:
    - **Включено** – со стороны оркестратора к устройству CPE применен назначенный шаблон CPE. Со стороны контроллера устройство CPE можно использовать для передачи трафика.
    - **Выключено** (в статусе **Ожидание**) – со стороны оркестратора к устройству CPE не применен назначенный шаблон CPE. Со стороны контроллера устройство CPE невозможно использовать для передачи трафика.
    - **Выключено** (в статусе **Зарегистрировано**) – оркестратор не отвечает на REST API-запросы, поступающие от устройства CPE. Со стороны контроллера устройству CPE заблокирована передача трафика через соединения.
  - **Подключение** – информация о том, подключено ли устройство CPE к контроллеру:
    - **Подключено**.
    - **Отключено**.

  Вы можете указать краткое описание устройства CPE в поле **Описание** и посмотреть выполняемые оркестратором задачи в таблице **Внеполосное управление**.
- **Мониторинг** – результаты мониторинга устройства CPE.
- **Проблемы** – проблемы, возникшие при работе устройства CPE. При наличии проблем рядом со вкладкой отображается красный восклицательный знак.
- **Шифрование** – параметры шифрования трафика.
- **Сервисные запросы** – сервисные запросы устройства CPE.
- **Теги** – теги для группировки устройств CPE.

- **Скрипты** – скрипты для дополнительной настройки устройства CPE.
- **SD-WAN** – параметры подключения устройства CPE к сети SD-WAN. На этой вкладке отображаются следующие вкладки:
  - **Основные параметры** – параметры подключения устройства CPE к оркестратору и контроллеру.
  - **Интерфейсы** – интерфейсы SD-WAN.
- **Топология** – топологические теги для построения соединений между устройствами CPE.
- **Сеть** – сетевые интерфейсы.
- **DHCP** – параметры DHCP.
- **Межсетевой экран** – параметры межсетевого экрана.
- **VRF** – виртуальные таблицы маршрутизации.
  - **BGP** – настройки параметров использования протокола BGP для обмена маршрутами между устройствами CPE и внешними сетевыми устройствами.
- **OSPF** – протокол OSPF для обмена маршрутами между устройствами CPE и внешними сетевыми устройствами. На этой вкладке отображаются следующие вкладки:
  - **Основные параметры** – основные параметры протокола OSPF.
  - **OSPF-области** – OSPF-области.
  - **OSPF-интерфейсы** – OSPF-интерфейсы.
- **Фильтры маршрутов** – параметры фильтрации маршрутов и пакетов трафика между устройствами CPE и внешними сетевыми устройствами. На этой вкладке отображаются следующие вкладки:
  - **Списки управления доступом** – списки управления доступом (ACLs).
  - **Списки префиксов** – списки префиксов (prefix lists).
  - **Карты маршрутизации** – карты маршрутизации (route maps).
- **PBR** – параметры маршрутизации на основе политик (PBR).
- **BFD** – протокол BFD для обнаружения ошибок маршрутизации между устройствами CPE и внешними сетевыми устройствами.
- **Статические маршруты** – статические маршруты.
- **Multicast** – параметры передачи multicast-трафика между устройствами CPE и внешними сетевыми устройствами с помощью протоколов PIM и IGMP. На этой вкладке отображаются следующие вкладки:
  - **Основные параметры** – основные параметры PIM.
  - **Интерфейсы** – multicast-интерфейсы.

- **VRRP** – протокол VRRP для обеспечения высокой доступности устройств CPE. На этой вкладке отображаются следующие вкладки:
  - **Экземпляры VRRP** – экземпляры VRRP.
  - **Группы экземпляров VRRP** – группы экземпляров VRRP.
- **CFM** – параметры функции Connectivity Fault Management (CFM).
- **UNI** – UNI на устройстве CPE.
- **Модемы** – параметры модемов устройства CPE.
- **Соединения** – параметры соединений.
- **Мультипутевая передача** – параметры путей.
- **Активация** – параметры двухфакторной аутентификации устройства CPE.
- **Деактивация** – параметры автоматического удаления и выключения устройства CPE.
- **Запись в журнал** – параметры журналов.
- **NetFlow** – основные параметры NetFlow.
- **NTP** – NTP-серверы для синхронизации времени.
- **Диагностическая информация** – запросы диагностической информации устройства CPE.
- **Утилиты** – утилиты для диагностики устройств CPE.

Добавление устройств CPE

Вам нужно добавить устройство CPE, если вы проводите его автоматическую регистрацию (ZTP). При добавлении устройства CPE необходимо указать идентификатор DPID, чтобы сопоставить добавленную запись с устройством CPE, которое вы подключите позже. Вы можете добавить устройство CPE для текущего экземпляра SD-WAN, тенанта или другого экземпляра SD-WAN. Возможно как добавление отдельного устройства, так и массовый импорт устройств с нужными параметрами из файла CSV.

Чтобы добавить устройство CPE:

1. Перейдите к добавлению устройства CPE одним из следующих способов:

   - Если вы хотите добавить устройство CPE текущему экземпляру SD-WAN, в меню перейдите в раздел **SD-WAN → CPE** и в верхней части страницы нажмите на кнопку **+ CPE**.

   - Если вы хотите добавить устройство CPE тенанту, в меню перейдите в раздел **Тенанты**, в блоке **Тенанты** выберите созданного тенанта и в блоке **[[ten.cpe.header]]** нажмите на кнопку **+ [[ten.cpe.device]]**.

   - Если вы хотите добавить устройство CPE другому экземпляру SD-WAN, в меню перейдите в подраздел **SD-WAN → Экземпляры SD-WAN**, нажмите на развернутый экземпляр SD-WAN и в верхней части области настройки в блоке **Действия** нажмите на кнопку **Создать**.

2. В открывшемся окне в поле **Имя** введите имя устройства CPE.

3. В поле **DPID** введите идентификатор DPID устройства CPE. Идентификатор DPID указан на коробке устройства CPE.

   Если у устройства CPE отсутствует идентификатор DPID, вы можете указать временный идентификатор DPID, например `temporary DPID`. Временный идентификатор DPID можно заменить на настоящий.

4. В раскрывающемся списке **Состояние** выберите состояние устройства CPE после регистрации:

   - **Включено** – применить к устройству CPE шаблон CPE и использовать для передачи трафика. Это значение выбрано по умолчанию.

   - **Выключено** – не применять к устройству CPE шаблон CPE.

5. При необходимости в поле **Описание** введите краткое описание устройства CPE.

6. Если вы добавляете устройство CPE экземпляру SD-WAN, в раскрывающемся списке **Тенант** выберите транспортного тенанта, которому вы хотите добавить устройство CPE. Устройство CPE подключается к контроллеру экземпляра SD-WAN, который был развернут для транспортного тенанта. Вы можете выбрать пул экземпляров SD-WAN.

7. В раскрывающемся списке **Клиентский тенант** выберите клиентского тенанта, которому вы хотите добавить устройство CPE. Клиентский тенант может управлять устройством CPE на своем портале самообслуживания.

8. Если вы хотите создать UNI на устройстве CPE с помощью шаблона UNI, в раскрывающемся списке **Шаблон UNI** выберите созданный шаблон UNI.

9. В раскрывающемся списке **Шаблон CPE** выберите созданный шаблон CPE, в соответствии с которым вы хотите настроить устройство CPE.

10. В раскрывающемся списке **Шаблон NetFlow** выберите созданный шаблон NetFlow, в соответствии с которым вы хотите настроить основные параметры NetFlow на устройстве CPE.

11. В раскрывающемся списке **Шаблон межсетевого экрана** выберите созданный шаблон межсетевого экрана, в соответствии с которым вы хотите настроить межсетевой экран устройства CPE.

12. Нажмите на кнопку **Далее** и в поле **Адрес** укажите адрес площадки устройства CPE. По мере ввода адреса вам предлагается выбрать адрес в раскрывающемся списке.

    Адрес отобразится на карте.

13. Нажмите на кнопку **Добавить**.

Устройство будет добавлено, перейдет в статус **Ожидание**, и вы получите один из следующих результатов:

- Если вы добавили устройство CPE для текущего экземпляру SD-WAN, устройство CPE отобразится в таблице.
- Если вы добавили устройство CPE тенанту, устройство CPE отобразится в блоке **[[ten.cpe.header]]**.
- Если вы добавили устройство CPE другому экземпляру SD-WAN, в новой вкладке бразуера откроется портал самообслуживания. Вы автоматически войдете на портал самообслуживания и перейдете в подраздел **CPE**. Устройство CPE отобразится в таблице.

Массовый импорт устройств CPE из файла CSV

При необходимости добавить одновременно большое количество устройств CPE вы можете использовать функцию массового импорта. Перед импортом устройств CPE вам необходимо указать их параметры в файле CSV. Файл CSV для импорта должен соответствовать следующим требованиям:

- Первая запись в CSV-файле содержит заголовки.
- Порядок заголовков может быть произвольным.
- Допустимое расширение импортируемого файла – `csv`.
- Максимальный размер файла – 10 485 760 байт.
- Максимальное количество записей в файле – 25001 (25000 записей + 1 строка с заголовками).

Если операция импорта происходит внутри тенанта, то клиентский и транспортный тенанты указываются оркестратором автоматически, а соответствующие значения, указанные в файле CSV, игнорируются.

Подробное описание столбцов файла см. в таблице в этой статье. Вы также можете скачать образец файла в окне импорта.

Чтобы импортировать устройства CPE из файла:

1. Подготовьте файл CSV для импорта.
2. В меню перейдите в раздел **SD-WAN → CPE**, в верхней части страницы с помощью значка ⌄ в правой части кнопки **+ CPE** откройте выпадающий список и выберите **Массовый импорт из CSV**.
3. В открывшемся окне выберите и загрузите в оркестратор подготовленный ранее файл CSV.

   После загрузки CSV-файла оркестратор выполняет проверку записей в файле.

4. Если в ходе проверки найдены ошибки, они перечисляются в окне импорта. Список ошибок разбит на вкладки в зависимости от типа ошибок:

   - **Неверный формат строк**
   - **Нет мониторинга**
   - **Не найден объект**
   - **Ошибки валидации**

   При наличии ошибок импорта исправьте их в файле и повторите попытку.

5. Если файл прошел проверку без ошибок, начнется процесс импорта. На все время проверки и импорта добавление устройство CPE блокируется (максимальное время блокировки – 30 секунд).

После успешного импорта будет выведено соответствующее сообщение с указанием количества добавленных устройств. Устройства будут добавлены, перейдут в статус **Ожидание** и отобразятся в таблице.

Описание содержимого столбцов файла CSV для пакетного импорта CPE

Имя столбца	Содержимое столбца	Процесс валидации	Наличие
`Name`	Имя устройства CPE. Произвольная строка текста.	Как при добавлении отдельного устройства CPE.	Обязательно
`MACAddress`	6 групп по 2 шестнадцатеричных числа, которые могут быть разделены дефисами, двоеточиями или не иметь разделителя. Примеры: • `DE-AD-BE-EF-11-22` • `DE:AD:BE:EF:11:22` • `DEADBEEF1122`	Полученное значение приводится к формату DPID: • добавляется 8000 в начало строки; • убираются разделители, если они имеются; • буквы `a-f` переводятся в верхний регистр, если они находятся в нижнем. Валидация полученного DPID как при добавлении отдельного устройства CPE.	Обязательно
`State`	Строка. Возможные значения: • `enabled` • `disabled`	Как при добавлении отдельного устройства CPE.	Обязательно
`Transport Tenant`	Имя транспортного тенанта.	По переданному значению выполняется поиск транспортного тенанта.	Обязательно
`CPE Template`	Имя шаблона CPE.	По переданному значению выполняется поиск шаблона CPE с владельцем, соответствующим тенанту, из которого осуществляется импорт CSV.	Обязательно
`NetFlow Template`	Имя шаблона NetFlow.	По переданному значению выполняется поиск шаблона NetFlow с владельцем, соответствующим тенанту, из которого осуществляется импорт CSV.	Обязательно
`Firewall Template`	Имя шаблона межсетевого экрана.	По переданному значению выполняется поиск шаблона межсетевого экрана с владельцем, соответствующим тенанту, из которого осуществляется импорт CSV.	Обязательно
`Description`	Описание устройства CPE. Произвольная строка текста.	Как при добавлении отдельного устройства CPE.	Необязательно
`Customer Tenant`	Имя клиентского тенанта.	По переданному значению выполняется поиск клиентского тенанта.	Необязательно
`UNI Template`	Имя шаблона UNI.	По переданному значению выполняется поиск шаблона UNI с владельцем, соответствующим тенанту, из которого осуществляется импорт CSV.	Необязательно

Генерация веб-адреса с базовыми параметрами устройства CPE

Для автоматической регистрации устройства CPE вам нужно сгенерировать веб-адрес с базовыми параметрами устройства CPE. Вы можете указать шаблон генерируемого веб-адреса при настройке подключения устройства CPE к оркестратору и контроллеру. Сгенерированный веб-адрес содержит следующую информацию:

- NTP-серверы;
- сетевые интерфейсы;
- параметры подключения устройства CPE к оркестратору и контроллеру и интерфейсы SD-WAN;
- сертификаты;
- параметры протокола BGP;
- токен при использовании двухфакторной аутентификации;
- виртуальные таблицы маршрутизации;
- справочники APN.

Максимальный размер веб-адреса с базовыми параметрами устройства CPE не должен превышать 64 КБ.

Чтобы сгенерировать веб-адрес с базовыми параметрами устройства CPE:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, для которого вы хотите сгенерировать веб-адрес с базовыми параметрами.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Получить конфигурационный URL**.

4. В открывшемся окне в выпадающем списке **Версия** укажите версию прошивки устройства CPE, для которого вы хотите сгенерировать веб-адрес с базовыми параметрами:

   - **Current**
   - **23.07**

5. Сохраните веб-адрес с базовыми параметрами устройства CPE одним из следующих способов:

   - Если вы хотите скопировать веб-адрес, нажмите рядом с ним на кнопку **Копировать**.
   - Если вы хотите сохранить веб-адрес в виде файла в формате HTML, нажмите рядом с ним на кнопку **Скачать в HTML**.

   Вам нужно подключить устройство администратора к LAN-порту устройства CPE и использовать сохраненный веб-адрес с базовыми параметрами для автоматической регистрации устройства CPE.

   Если вам нужно установить сертификаты на устройстве CPE с версией прошивки 23.07, воспользуйтесь инструкцией, описанной в статье Сценарий: установка сертификатов на устройстве CPE с версией прошивки 23.07.

Регистрация устройства CPE вручную

Вам нужно вручную зарегистрировать устройство CPE в веб-интерфейсе при повторной регистрации устройства CPE. При регистрации не требуется подключаться к облачным сервисам "Лаборатории Касперского".

Чтобы зарегистрировать устройство CPE вручную:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, которое вы хотите зарегистрировать вручную.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Зарегистрировать**.

4. В открывшемся окне в раскрывающемся списке **Состояние** выберите состояние устройства CPE после регистрации:

   - **Включено** – применить к устройству CPE шаблон CPE и использовать для передачи трафика. Это значение выбрано по умолчанию.
   - **Выключено** – не применять к устройству CPE шаблон CPE.

5. При необходимости в поле **Описание** введите краткое описание устройства CPE.

6. В раскрывающемся списке **Тенант** выберите транспортного тенанта, которому вы хотите добавить устройство CPE. Устройство CPE подключается к контроллеру экземпляра SD-WAN, который был развернут для транспортного тенанта. Вы можете выбрать пул экземпляров SD-WAN.

7. В раскрывающемся списке **Клиентский тенант** выберите клиентского тенанта, которому вы хотите добавить устройство CPE. Клиентский тенант может управлять устройством CPE на своем портале самообслуживания.

8. Если вы хотите создать UNI на устройстве CPE с помощью шаблона UNI, в раскрывающемся списке **Шаблон UNI** выберите созданный шаблон UNI.

9. В раскрывающемся списке **Шаблон CPE** выберите созданный шаблон CPE, в соответствии с которым вы хотите настроить устройство CPE.

10. В раскрывающемся списке **Шаблон NetFlow** выберите созданный шаблон NetFlow, в соответствии с которым вы хотите настроить основные параметры NetFlow на устройстве CPE.

11. В раскрывающемся списке **Шаблон межсетевого экрана** выберите созданный шаблон межсетевого экрана, в соответствии с которым вы хотите настроить межсетевой экран устройства CPE.

12. Нажмите на кнопку **Далее** и в поле **Адрес** укажите адрес площадки устройства CPE. По мере ввода адреса вам предлагается выбрать адрес в раскрывающемся списке.

    Адрес отобразится на карте.

13. Нажмите на кнопку **Зарегистрировать**.

Статус устройства CPE изменится сначала на **Регистрация**, затем на **Зарегистрировано**.

Отмена регистрации устройства CPE

Чтобы отменить регистрацию устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, регистрацию которого вы хотите отменить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Отменить регистрацию**.

4. В открывшемся окне подтверждения нажмите на кнопку **Отменить регистрацию**.

Регистрация устройства CPE будет отменена, и статус устройства CPE изменится на **Ожидание**.

Указание адреса устройства CPE

Чтобы указать адрес устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, адрес которого вы хотите указать.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Указать адрес**.

4. В открывшемся окне введите адрес площадки устройства CPE. По мере ввода адреса вам будет предложено выбрать адрес в раскрывающемся списке.

   Адрес отобразится на карте.

5. Нажмите на кнопку **Сохранить**.

Адрес устройства CPE будет указан.

Включение и выключение устройства CPE

При включении устройства CPE к нему применяется шаблон CPE. Выключенные устройства CPE невозможно использовать для передачи трафика.

Чтобы включить или выключить устройство CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, которое вы хотите включить или выключить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Включить** или **Выключить**.

Устройство CPE будет включено или выключено.

Перезагрузка устройства CPE

Чтобы перезагрузить устройство CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, которое вы хотите перезагрузить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Перезагрузить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Перезагрузить**.

Устройство CPE будет перезагружено.

Выключение питания устройства CPE

Вы можете выключить питание устройства CPE в веб-интерфейсе оркестратора, или отключив кабель питания от устройства CPE. При выключении питания в веб-интерфейсе оркестратора в оперативную систему устройства CPE отправляется команда `shutdown`.

Чтобы выключить питание устройства CPE в веб-интерфейсе оркестратора:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, питание которого вы хотите выключить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Выключить питание**.

4. В открывшемся окне подтверждения нажмите на кнопку **Выключить питание**.

Питание устройства CPE будет выключено.

Подключение к консоли устройства CPE

Чтобы подключиться к консоли устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, к консоли которого вы хотите подключиться.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Открыть SSH-консоль**.

В новой вкладке браузера откроется окно консоли устройства CPE.

Просмотр пароля устройства CPE

Чтобы посмотреть пароль устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, пароль которого вы хотите посмотреть.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Показать пароль**.

Откроется окно с паролем устройства CPE.

Экспорт параметров подключения к оркестратору и контроллеру и интерфейсов SD-WAN из устройства CPE

Чтобы экспортировать параметры подключения к оркестратору и контроллеру интерфейсы SD-WAN из устройства CPE:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, из которого вы хотите экспортировать параметры подключения к оркестратору и контроллеру и интерфейсы SD-WAN.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Экспортировать параметры SD-WAN**.

На вашем локальном устройстве будет сохранен файл в формате JSON с именем <Имя шаблона>sdwan-config.

Экспорт сетевых интерфейсов из устройства CPE

Чтобы экспортировать сетевые интерфейсы из устройства CPE:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, из которого вы хотите экспортировать сетевые интерфейсы.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Вверху в блоке **Действия** нажмите на кнопку **Экспортировать сетевые интерфейсы**.

На ваше локальное устройство сохранится файл в формате JSON и именем <Имя шаблона>-network-config.

Изменение идентификатора DPID устройства CPE

Вам может потребоваться изменить идентификатор DPID в следующих сценариях:

- развертывание устройства vCPE на платформе виртуализации VMware с автоматической регистрацией.
- замена существующего зарегистрированного устройства CPE на новое устройство CPE с сохранением прежней сетевой конфигурации (например, при выходе устройства из строя).

Чтобы изменить идентификатор DPID устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, идентификатор DPID которого вы хотите изменить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Изменить DPID**.

4. В открывшемся окне введите новый идентификатор DPID устройства CPE.

5. Нажмите на кнопку **Сохранить**.

Идентификатор DPID устройства CPE будет изменен.

Изменение параметров устройств CPE

При необходимости вы можете изменить параметры устройства CPE. Доступно как мгновенное применение измененных параметров, так и отложенное применение параметров через планировщик задач.

Чтобы изменить параметры устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, параметры которого вы хотите изменить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выбрав нужные вкладки с параметрами устройства CPE, измените необходимые параметры.

4. Выберите нужный вариант сохранения параметров:

- Если вы хотите, чтобы изменения параметров применились мгновенно, нажмите на кнопку **Сохранить**.

  Параметры устройства CPE будут сохранены.

- Если вы ходите запланировать применение параметров на определенное время:

  1. С помощью значка ⌄ в правой части кнопки **Сохранить** откройте меню режимов сохранения и выберите **Запланированное сохранение**.

     Откроется боковая панель создания задачи.

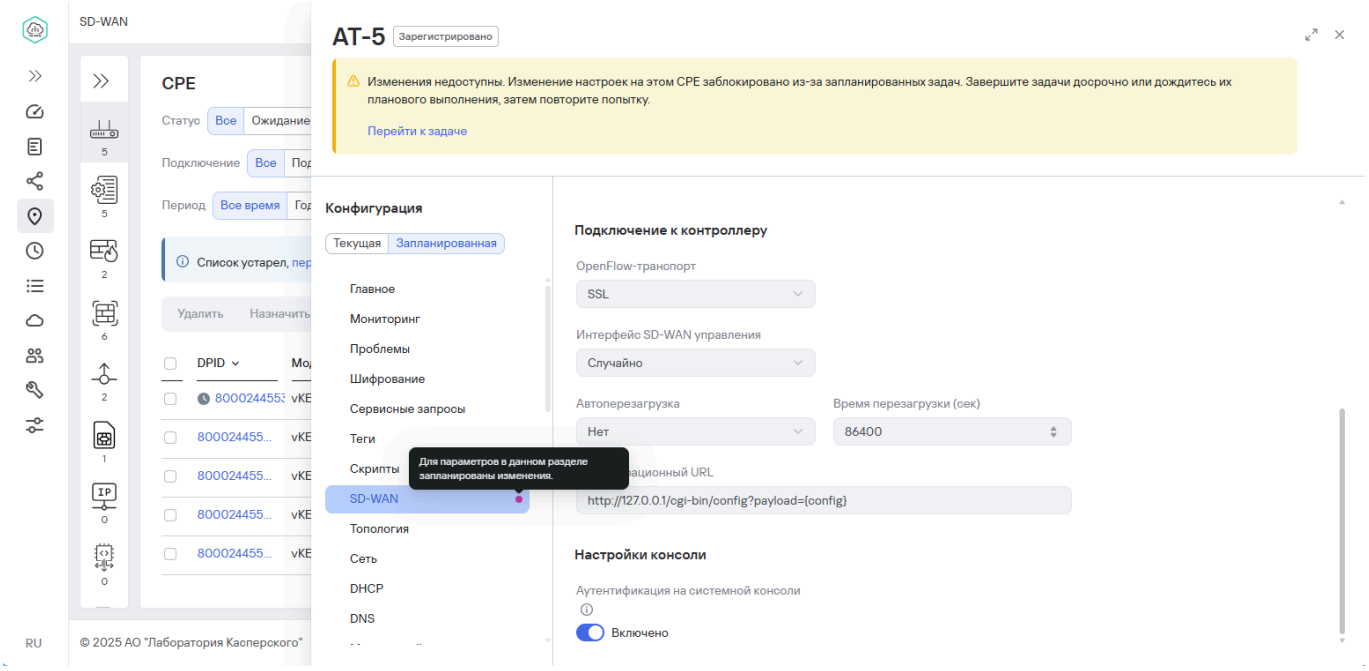
  2. В поле **Запланированное время выполнения задачи** введите дату и время выполнения задачи. По умолчанию указана дата и время, когда вы начали создавать задачу.

  3. В поле **Имя задачи** при необходимости введите имя задачи. По умолчанию в этом поле введено имя Schedule settings update.

  4. Нажмите на кнопку **Запланировать**.

  Задача запланированного изменения параметров устройства CPE будет создана. Вы можете посмотреть статус задачи в таблице **Планировщик**.

  Устройство CPE, на котором запланированы изменения, отображается в таблице в разделе **SD-WAN → CPE** со значком 🕒 рядом с его DPID. В области настройки устройства CPE появляются вкладки для просмотра текущей и запланированной конфигурации устройства. Разделы с настройками параметров, в которых запланированы изменения в рамках созданной задачи на изменение, выделяются визуально. Изменение параметров устройства CPE и используемого им шаблона CPE становится невозможным до завершения запланированной задачи. Вы можете перейти к задаче, нажав на **Перейти к задаче**, и завершить досрочно либо удалить ее.



Отображение CPE с запланированными изменениями

Удаление устройств CPE

При удалении устройства CPE автоматически удаляются все созданные на нем сервисные интерфейсы.

Удаленные устройства CPE невозможно восстановить.

Чтобы удалить устройства CPE:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Если вы хотите удалить отдельное устройство CPE, выполните следующие действия:

   a. Нажмите на устройство CPE, которое вы хотите удалить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

   b. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

3. Если вы хотите удалить несколько устройств CPE, выполните следующие действия:

   a. Установите флажки рядом с устройствами CPE, которые вы хотите удалить.

   b. В верхней части таблицы нажмите на кнопку **Действия** → **Удалить**.

4. В открывшемся окне подтверждения выберите способ удаления устройства CPE:

   - **Удалить, отменить регистрацию и сбросить пароль** – удалить устройство CPE из веб-интерфейса оркестратора. При включении устройство CPE повторно подключается к оркестратору и отображается в веб-интерфейсе оркестратора со статусом **Неизвестно**.

   - **Сбросить до заводских параметров** – удалить устройство CPE из веб-интерфейса оркестратора и сбросить параметры устройства CPE до заводских значений. При включении устройство CPE не подключается к оркестратору и не отображается в веб-интерфейсе оркестратора.

   - **Удалить принудительно** – удалить устройство CPE из веб-интерфейса оркестратора. Вы можете выбрать это значение, чтобы удалить недоступное устройство CPE или лишнюю запись из веб-интерфейса оркестратора.

5. Нажмите на кнопку **Удалить**.

Устройства CPE будут удалены и перестанут отображаться в таблице.

Двухфакторная аутентификация устройства CPE

Вы можете использовать *двухфакторную аутентификацию*, чтобы безопасно зарегистрировать устройство CPE. При включенной двухфакторной аутентификации в базу данных оркестратора записывается токен (ключ безопасности), который затем вы помещаете на устройство CPE при регистрации с использованием технологии Zero Touch Provisioning. Регистрация проходит успешно, если при автоматическом подключении устройства CPE к оркестратору помещенный на устройство CPE токен совпадает с токеном в базе данных оркестратора.

Вы не можете использовать двухфакторную аутентификацию для уже зарегистрированного устройства CPE.

Чтобы использовать двухфакторную аутентификацию для устройства CPE:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, для которого вы хотите использовать двухфакторную аутентификацию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Активация**.

   Отобразятся параметры двухфакторной аутентификации.

4. В раскрывающемся списке **Двухфакторная аутентификация** выберите **Включено**. Значение по умолчанию: **Выключено**.

5. Если вы хотите сгенерировать новый токен, нажмите на кнопку **Сгенерировать** под полем **Токен**.

6. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Работа с сертификатами

При взаимодействии с оркестратором устройство CPE проверяет, можно ли доверять сертификатам оркестратора для предотвращения MITM-атак. По умолчанию устройство CPE доверяет публичным центрам сертификации.

Если для оркестратора используются сертификаты, подписанные пользовательским центром сертификации, вам нужно загрузить их в веб-интерфейс оркестратора и установить на устройствах CPE. Поддерживаются одиночные корневые сертификаты и цепочки сертификатов, состоящие из одного корневого сертификата и нескольких промежуточных сертификатов.

За 30 дней до окончания срока действия сертификата уведомление об этом отображается при входе в веб-интерфейс оркестратора.

Вы можете посмотреть таблицу сертификатов в разделе **SD-WAN → Сертификаты**. Информация о сертификатах отображается в следующих столбцах таблицы:

- **Общее имя** – доменное имя или имя хоста, для которого предназначен сертификат.
- **Организация** – имя организации, выпустившей сертификат.
- **Распространить на CPE** – флажок для установки сертификата на устройствах CPE. Сертификаты, рядом с которыми установлены флажки, устанавливаются на устройствах CPE в следующих случаях:
  - при автоматической регистрации (ZTP) устройства CPE;
  - при перезагрузке устройства CPE;
  - при ручной установке сертификатов на устройстве CPE.

  При неправильном выборе сертификатов устройство CPE может перестать доверять сертификату оркестратора и отключиться от него.
- **От** – дата начала действия сертификата.
- **До** – дата окончания действия сертификата.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Загрузка сертификата в веб-интерфейс оркестратора

Чтобы загрузить сертификат в веб-интерфейс оркестратора:

1. В меню перейдите в раздел **SD-WAN → Сертификаты**.

   Отобразится таблица сертификатов.
2. В верхней части страницы нажмите на кнопку **+ Сертификат**.
3. Укажите путь к файлу сертификата в формате PEM. Максимальный размер файла: 16 КБ.

Сертификат будет загружен и отобразится в таблице. Отобразится сообщение *Сертификат <имя сертификата> загружен*.

Ручная установка сертификатов на устройствах CPE

Чтобы установить сертификаты на устройствах CPE:

1. В меню перейдите в раздел **SD-WAN** → **Сертификаты**.

   Отобразится таблица сертификатов.

2. Установите флажки **Распространить на CPE** рядом с загруженными сертификатами, которые вы хотите установить на устройствах CPE.

3. Нажмите на кнопку **Применить на CPE**.

Сертификаты будут установлены на устройствах CPE. Отобразится сообщение *Сертификаты применены к CPE*.

Сценарий: установка сертификатов на устройстве CPE с версией прошивки 23.07

Вы можете установить корневой сертификат или цепочку сертификатов, подписанных пользовательским центром сертификации, на устройстве CPE с версией прошивки 23.07.

Версия прошивки 23.07 полноценно не поддерживается текущей версией оркестратора, поэтому при использовании этой версии прошивки могут возникнуть технические неполадки. Мы рекомендуем обновить прошивки всех устройств CPE до последней версии.

Сценарий установки сертификатов на устройствах CPE с версией прошивки 23.07 состоит из следующих этапов:

1. **Загрузка сертификатов в веб-интерфейс оркестратора**

   Загрузите сертификаты в веб-интерфейс оркестратора.

2. **Генерация веб-адреса с базовыми параметрами устройства CPE**

   Сгенерируйте веб-адрес с базовыми параметрами устройства CPE, при этом выполнив следующие действия:

   1. В раскрывающемся списке **Версия** выберите **23.07**.

      Будут сгенерированы конфигурационные веб-адреса для каждого из загруженных сертификатов.

   2. Нажмите на кнопку **Копировать** рядом со всеми сгенерированными веб-адресами.

   3. Сохраните скопированные веб-адреса.

3. **Установка сертификатов на устройстве CPE**

   Выполните следующие действия:

   1. Подключите устройство администратора к LAN-порту устройства CPE.

Устройство администратора получит IP-адрес и IP-адрес шлюза по умолчанию по протоколу DHCP. Полученный IP-адрес шлюза по умолчанию является IP-адресом устройства CPE.

2. С устройства администратора поочередно перейдите по каждому сгенерированному веб-адресу.

Устройство CPE будет перезагружаться после установки каждого сертификата. Учтите, что после перезагрузки устройство CPE может получить новый IP-адрес, поэтому вам может потребоваться изменить скопированный ранее веб-адрес для установки следующего сертификата.

Экспорт сертификата

Чтобы экспортировать сертификат:

1. В меню перейдите в раздел **SD-WAN** → **Сертификаты**.

   Отобразится таблица сертификатов.

2. Нажмите на сертификат, который вы хотите экспортировать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Экспортировать**.

На ваше локальное устройство сохранится файл сертификата в формате PEM.

Удаление сертификатов

Удаленные сертификаты невозможно восстановить.

Чтобы удалить сертификаты:

1. В меню перейдите в раздел **SD-WAN** → **Сертификаты**.

   Отобразится таблица сертификатов.

2. Если вы хотите удалить отдельный сертификат, выполните следующие действия:

   a. Нажмите на сертификат, который вы хотите удалить.

      Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

   b. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

3. Если вы хотите удалить несколько сертификатов, выполните следующие действия:

   a. Установите флажки рядом с сертификатами, которые вы хотите удалить.

   b. В верхней части таблицы нажмите на кнопку **Действия** → **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Сертификаты будут удалены и перестанут отображаться в таблице.

Работа со справочниками APN

Для просмотра таблицы справочников APN вам нужно в меню перейти в раздел **SD-WAN → Справочники APN**. По умолчанию на портале администратора создан справочник APN **DefaultAPNDir**.

Информация о справочниках APN отображается в следующих столбцах таблицы:

- **Имя** – имя справочника APN.
- **Использование** – использование справочника APN устройствами CPE:
  - **Да**.
  - **Нет**.
- **Владелец** – тенант, к которому относится справочник APN.
- **Изменено** – дата и время последнего изменения параметров справочника APN.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание справочника APN

Чтобы создать справочник APN:

1. В меню перейдите в раздел **SD-WAN → Справочники APN**.

   Отобразится таблица справочников APN.

2. Если вы хотите добавить справочник APN вручную:

   a. В верхней части страницы нажмите на кнопку **+ Создать**.

   Откроется окно добавления справочника APN с таблицей записей APN.

   b. В поле **Имя** введите имя справочника APN.

   c. Добавьте одну или несколько записей APN с помощью кнопки **Добавить**. Для каждой записи заполните поля:

   - **PLMN**: PLMN-идентификатор оператора связи. Первые три цифры идентификатора PLMN являются кодом страны (MCC, англ. Moblie Country Code), следующие две или три цифры – кодом мобильной сети (MNC, англ. Mobile Network Code). Например, для сети "Вымпелком" на территории Российской Федерации PLMN=25099: MCC = 250 (РФ), MNC = 99 (Вымпелком).

     Обязательный параметр.

   - **APN**: строка APN от оператора связи. Допустимы символы: `[0-9A-Za-z-.]`. Строка должна начинаться и заканчиваться с буквы или цифры. Может быть пустой строкой. Максимальная длина – 100 символов.

     Обязательный параметр.

   - **Имя пользователя APN**: имя пользователя APN для аутентификации у оператора. Максимальная длина – 32 символа. Допустимые символы: `[0-9A-Za-z-._#$%*]`.

     Необязательный параметр.

   - **Пароль APN**: пароль APN для аутентификации у оператора. Максимальная длина – 32 символа. Допустимые символы: `[0-9A-Za-z~`!@#$%^&*()_-+={[}]|\:;"'<,>.?/]`.

     Необязательный параметр.

   Для удаления записи APN нажмите рядом с ней на кнопку **Удалить**.

   d. Нажмите на кнопку **Создать**.

3. Если вы хотите добавить справочник APN из файла:

   a. В верхней части страницы нажмите на кнопку **Загрузить из файла**.

   b. В открывшемся окне выберите файл для импорта справочника APN в формате json. Файл должен иметь следующую структуру:

```
{
        "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": "********"}
    ]
}
```

Справочник APN будет создан и отобразится в таблице.

Просмотр и сброс сессий на устройствах CPE

Устройства CPE отслеживают и хранят информацию о входящих и исходящих соединениях в виде сессий. Сессия представляет собой набор связанных атрибутов, которые позволяют объединять отдельные пакеты в одну логическую сущность и отслеживать ее состояние.

Вы можете загружать и просматривать список сессий нужного устройства CPE с помощью веб-интерфейса оркестратора, например, чтобы быстро диагностировать проблемы с подключением пользователей, анализировать сетевую активность или отслеживать использование ресурсов CPE в реальном времени. Вы также можете сбросить список сессий на устройстве.

Чтобы просмотреть или сбросить список сессий устройства CPE:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, список сессий которого вы хотите просмотреть.

3. Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

4. Перейдите в раздел **Межсетевой экран** и выберите вкладку **Сессии**.

   Отобразится таблица сессий. По умолчанию таблица сессий пустая, т.к. сессии не загружены с устройства CPE.

5. Запросите сессии с устройства, нажав на кнопку **Запросить с CPE**.

   Дождитесь получения списка сессий с устройства CPE.

   Информация о сессиях отображается в следующих столбцах таблицы:

   - **Протокол**
   - **Время (сек.)**
   - **Состояние**
   - **IP источника**
   - **Исходящий порт**
   - **IP назначения**
   - **Порт назначения**
   - **Ответный IP ист.**
   - **Ответный порт ист.**
   - **Ответный IP назн.**
   - **Ответный порт назн.**
   - **Исходящих пакетов**
   - **Входящих пакетов**
   - **Исходящий трафик (байт)**
   - **Входящий трафик (байт)**
   - **Флаг сессии**
   - **Метка**

   Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

6. Если вы хотите отфильтровать отображаемые в таблице сессии, выполните следующие действия:

   a. Нажмите на значок фильтра ▽ в правом углу панели действий над таблицей.

      Откроется окно создания фильтра.

   b. Добавьте фильтры по нужным полям: для каждого фильтра нажмите на кнопку **Добавить**, выберите поле и укажите значение для фильтрации.

   c. Примените фильтр с помощью кнопки **Применить.**

   Сессии будут отображаться в таблице с учетом примененного фильтра.

7. Если вы хотите сбросить список сессий на устройстве, нажмите на кнопку **Сбросить сессии на CPE**.

   Появится предупреждение:

   > Очистка сессий может привести ко временной потере связи с контроллером и перестроению соединений этого CPE и, как следствие, вызвать временную потерю трафика.

   Подтвердите сброс сессий, нажав **Очистить таблицу сессий**.

Автоматическое удаление и выключение устройств CPE

Вы можете указать в шаблоне CPE или на устройстве CPE время, по прошествии которого устройство CPE удаляется или выключается (англ. disable) в случае разрыва управляющей сессии с контроллером. Обе функции используются для предотвращения краж устройств CPE. Функция автоматического удаления также используется для очистки веб-интерфейса оркестратора от устаревших записей. По умолчанию обе функции выключены.

Время автоматического удаления или выключения, указанное в шаблоне CPE, автоматически используется для всех устройств CPE, которые используют шаблон CPE.

Чтобы настроить автоматическое удаление и выключение устройств CPE:

1. Перейдите к настройке автоматического удаления и выключения одним из следующих способов:

   - Если вы хотите настроить автоматическое удаление и выключение в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Деактивация**.

   - Если вы хотите настроить автоматическое удаление и выключение на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Деактивация** и установите флажки **Переопределить**.

   Отобразятся параметры автоматического удаления и выключения устройства CPE.

2. Включите автоматическое удаление устройства CPE:

   a. Установите флажок **Включить** рядом с полем **Время удаления (сек.)**.

   b. В поле **Время удаления (сек.)** введите время в секундах, по прошествии которого устройство CPE удаляется при отсутствии связи с контроллером. Диапазон значений: от 60 до 31 536 000. Введенное значение не должно быть ниже значения, которое вы указываете для автоматического выключения.

3. Включите автоматическое выключение устройства CPE:

   a. Установите флажок **Включить** рядом с полем **Время выключения (сек.)**.

   b. В поле **Время выключения (сек.)** введите время в секундах, по прошествии которого устройство CPE выключается при отсутствии связи с контроллером. Диапазон значений: от 60 до 31 536 000. Введенное значение не должно быть выше значения, которое вы указываете для автоматического удаления.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Группировка устройств CPE с помощью тегов

Теги описывают параметры устройства CPE, такие как модель, версию прошивки и адрес расположения. Когда вы добавляете устройство CPE, ему автоматически назначаются теги, описывающие модель и тенанта, которому было добавлено устройство CPE.

Вы можете использовать теги для группировки устройств CPE и выполнения действий с группами. Например, вы можете назначить одинаковый тег устройствам CPE, которые находятся на одной площадке, после чего обновить на них прошивку.

Для назначения тега устройство CPE должно находиться в статусе **Зарегистрировано**. Одному устройству CPE невозможно назначить два одинаковых тега.

Назначение тега устройствам CPE

Чтобы назначить тег устройствам CPE:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Если вы хотите назначить тег отдельному устройству CPE, выполните следующие действия:

   a. Нажмите на устройство CPE, которому вы хотите назначить тег.

      Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

   b. Выберите вкладку **Теги**.

      Отобразятся назначенные теги.

   c. Введите тег и нажмите на значок назначения +.

   d. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

3. Если вы хотите назначить тег нескольким устройствам CPE, выполните следующие действия:

   a. Установите флажки рядом с устройствами CPE, которым вы хотите назначить тег.

   b. В верхней части таблицы нажмите на кнопку **Действия** → **Назначить теги**.

   c. В открывшемся окне введите тег и нажмите на значок назначения +.

   d. Нажмите на кнопку **Добавить**.

Тег будет назначен устройствам CPE.

Удаление тега устройств CPE

Чтобы удалить тег устройств CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Если вы хотите удалить тег отдельного устройства CPE, выполните следующие действия:

   a. Нажмите на устройство CPE, тег которого вы хотите удалить.

      Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

   b. Выберите вкладку **Теги**.

      Отобразятся назначенные теги.

   c. Нажмите на значок удаления ✕ рядом с тегом, который вы хотите удалить.

   d. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

3. Если вы хотите удалить тег нескольких устройств CPE, выполните следующие действия:

   a. Установите флажки рядом с устройствами CPE, тег которых вы хотите удалить.

   b. В верхней части таблицы нажмите на кнопку **Действия → Удалить теги**.

   c. В открывшемся окне удалите теги одним из следующих способов:

      - Нажмите на значок удаления ✕ рядом с тегом, который вы хотите удалить.
      - Введите тег, который вы хотите удалить, и выберите его в раскрывающемся списке.

   d. Нажмите на кнопку **Удалить**.

Тег устройств CPE будет удален.

Настройка журналов на устройствах CPE

Генерируемые на устройствах CPE журналы хранятся локально или отправляются на внешний syslog-сервер. При локальном хранении журналов вы можете указать их максимальный размер. До отправления на внешний syslog-сервер журналам может назначаться указанный вами префикс.

Для просмотра локального журнала на устройстве CPE вам нужно запросить диагностическую информацию.

Вы можете указать параметры журналов в шаблоне CPE или на устройстве CPE. Параметры журналов, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

Чтобы настроить журналы на устройствах CPE:

1. Если вы хотите, чтобы устройство CPE отправляло журналы на внешний syslog-сервер в зашифрованном виде, предварительно загрузите на устройство CPE CA-сертификат сервера syslog:

   1. Откройте вкладку **SD-WAN → Сертификаты**, нажмите кнопку **+ Добавить**, в открывшейся форме нажмите **Загрузить** и выберите файл сертификата.

      Загруженный сертификат появится в таблице сертификатов.

   2. В таблице сертификатов установите флажок **Распространить на CPE** для добавленного сертификата.

   3. Нажмите на кнопку **Применить на CPE**.

2. Перейдите к настройке журналов одним из следующих способов:

   - Если вы хотите настроить журналы в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE, выберите раздел **Запись в журнал** и в области настройки откройте вкладку **Общие**.

   - Если вы хотите настроить журналы на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите раздел **Запись в журнал**, в области настройки откройте вкладку **Общие** и включите переключатель **Переопределить**.

   Отобразятся параметры журналов.

3. В поле **IP/FQDN** введите IP-адрес или полное доменное имя syslog-сервера.

   Если для отправки syslog-сообщений необходимо использовать зашифрованное соединение, и соответствующий CA-сертификат был выписан на доменное имя, то в поле **IP/FQDN** необходимо указать полное доменное имя. Это доменное имя должно разрешаться через DNS-сервер, указанный при настройке DNS на устройстве CPE.

4. В поле **Порт** введите номер порта syslog-сервера. Диапазон значений: от 0 до 65 353.

5. В раскрывающемся списке **Протокол** выберите протокол для передачи журналов на syslog-сервер:

   - **UDP**. Это значение выбрано по умолчанию.
   - **TCP**.
   - **TLS**. Выберите это значение, если вы хотите, чтобы устройство CPE отправляло журналы на внешний syslog-сервер в зашифрованном виде.

     Параметры настройки алгоритма шифрования (cipher) между клиентом и сервером syslog определяются сервером syslog. На устройствах CPE поддерживаются следующие версии алгоритма шифрования (cipher) и версий TLS:

     - `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=any Au=any 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. В поле **Размер файлов (КБ)** введите максимальный размер журналов на устройстве CPE в килобайтах. Диапазон значений: от 64 до 2048. Значение по умолчанию: `64`. Если максимальный размер журналов превышается, новые журналы перезаписывают наиболее старые журналы.

7. Если вы хотите, чтобы устройство CPE добавляло к записям в журнал префикс, укажите его в поле **Префикс для журналов**. Максимальная длина префикса – 256 символов.

8. При необходимости настройте фильтрацию отправляемых на сервер syslog сообщений с помощью поля **Фильтр сообщений**. При использовании фильтра сообщений на сервер syslog будут отправляться только записи журналов, которые содержат указанные в фильтре строки. Вы можете указать до десяти отдельных строк. Между строками действует логическое ИЛИ. Разрешенные символы для строк фильтра:

   - Буквы латинского алфавита в верхнем регистре (A-Z)
   - Буквы латинского алфавита в нижнем регистре (a-z)
   - Цифры (0-9)
   - Специальные символы (: - . _)
   - Пробел

9. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с модемами

Данный функционал поддерживается не всеми моделями. За консультацией рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Устройство CPE может иметь до четырех модемов для подключения к сети оператора связи. Для просмотра таблицы модемов вам нужно перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Модемы**. Информация о модемах отображается в следующих столбцах таблицы:

- **Имя** – имя модема.
- **IP** – IP-адрес модема.
- **Подсеть** – подсеть, к которой подключен модем.
- **Шлюз** – шлюз, к которому подключен модем.
- **DNS 1**, **DNS 2** – DNS-серверы, которые использует модем.
- **Сигнал** – уровень сигнала модема.
- **Формат данных** – протокол передачи данных на модеме.
- **Регистрация** – статус регистрации модема.
- **Сеть** – сеть, к которой подключен модем.
- **Страна** – страна, в которой зарегистрирован модем.
- **PLMN MCC** – мобильный код страны (англ. Mobile Country Code).

- **PLMN MNC** – мобильный код сети (англ. Mobile Network Code).
- **Роуминг** – на модеме используется роуминг:
  - **Да**.
  - **Нет**.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Обновление прошивки

Новые версии программного обеспечения устройств CPE распространяются специалистами "Лаборатории Касперского" в виде прошивок (англ. firmware). Поддерживаются прошивки на основе следующих программных коммутаторов:

- Open vSwitch (OVS) – реализация программного коммутатора с обработкой пакетов на уровне ядра. Этот тип коммутатора подходит для большинства устройств и выбран по умолчанию.
- Switch Operating System (SWOS) – альтернативная реализация программного коммутатора с обработкой пакетов на основе DPDK. Может демонстрировать увеличенную производительность благодаря обработке пакетов в обход ядра.

Вы можете скачать архив с прошивкой в формате TAR.GZ из директории /cpe комплекта поставки.

Существует три способа обновления прошивки на устройстве CPE:

- Обновление прошивки на устройстве CPE вручную без использования веб-интерфейса оркестратора.
- Запланированное обновление прошивки на выбранных устройствах CPE. В этом случае вы загружаете прошивку в веб-интерфейс оркестратора, выбираете устройства CPE, на которых хотите обновить прошивку, после чего обновляете прошивку. В планировщике задач автоматически создается задача по обновлению прошивки.
- Запланированное обновление прошивки на устройствах CPE с указанными тегами. В этом случае вы загружаете прошивку в веб-интерфейс оркестратора, назначаете теги устройствам CPE, на которых хотите обновить прошивку, после чего создаете задачу по обновлению прошивки в планировщике задач. При создании задачи требуется указать назначенные устройствам CPE теги.

В процессе обновления прошивки устройство CPE перезагружается.

Вы можете посмотреть таблицу загруженных в веб-интерфейс оркестратора прошивок в разделе **SD-WAN → Прошивка**. Информация о прошивках отображается в следующих столбцах таблицы:

- **Версия** – версия прошивки.
- **Размер (МБ)** – размер архива с прошивкой в мегабайтах.
- **SHA256** – хеш-сумма прошивки.
- **Архитектура** – архитектура набора команд (англ. instruction set architecture, ISA) прошивки.

- **Дата выпуска** – дата выпуска прошивки.
- **Модель** – модель устройств CPE, с которой совместима прошивка.
- **Тип коммутатора** – тип программного коммутатора, на основе которого сделана прошивка (OVS или SWOS).

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Обновление прошивки на устройстве CPE вручную

При выполнении этой инструкции вам потребуется ввести учетные данные устройства CPE. После регистрации пароль по умолчанию устройства CPE автоматически изменится. Вы можете посмотреть пароль устройства CPE в веб-интерфейсе оркестратора.

Чтобы обновить прошивку на устройстве CPE вручную:

1. Скачайте архив с прошивкой из директории /cpe комплекта поставки на устройство администратора, например на ноутбук. Если вы не знаете, какую версию прошивки требуется установить на устройстве CPE, используйте таблицу соответствия моделей устройств CPE версиям прошивок.
2. Подключите устройство администратора к LAN-порту устройства CPE.

   Устройство администратора получит IP-адрес шлюза по умолчанию по протоколу DHCP. Полученный IP-адрес шлюза по умолчанию является IP-адресом устройства CPE.
3. Подключитесь к устройству CPE по протоколу SCP, например с помощью программы WinSCP. Для подключения по протоколу SCP вам нужно указать IP-адрес и ввести учетные данные устройства CPE.
4. Поместите архив с прошивкой в директорию /tmp.
5. Подключитесь к устройству CPE по протоколу SSH. Для подключения по протоколу SSH вам нужно указать IP-адрес и ввести учетные данные устройства CPE.
6. Перейдите в директорию /tmp, выполнив команду:

   ```
   cd /tmp/
   ```
7. Обновите прошивку на устройстве CPE одним из следующих способов:
   - Если вы хотите оставить параметры устройства CPE без изменений после обновления прошивки, выполните команду:

     ```
     sysupgrade knaas-<имя архива с прошивкой>
     ```
   - Если вы хотите сбросить параметры устройства CPE до заводских значений после обновления прошивки, выполните команду:

     ```
     sysupgrade -n knaas-cpe<имя архива с прошивкой>
     ```

   При сбросе параметров до заводских значений устройство CPE отключается от оркестратора. Для повторного подключения устройства CPE к оркестратору вам нужно автоматически зарегистрировать устройство CPE (ZTP).

На устройстве CPE будет установлена новая версия прошивки, после чего устройство CPE перезагрузится. По умолчанию IP-адрес устройства CPE не изменяется, и на LAN-портах включен протокол DHCP.

Загрузка прошивки в веб-интерфейс оркестратора

Чтобы загрузить прошивку в веб-интерфейс оркестратора:

1. Скачайте архив с прошивкой из директории /cpe комплекта поставки на ваше локальное устройство. Если вы не знаете, какую версию прошивки требуется установить на устройстве CPE, используйте таблицу соответствия моделей устройств CPE версиям прошивок.

2. В меню перейдите в раздел **SD-WAN** → **Прошивка**.

   Отобразится таблица прошивок.

3. В верхней части страницы нажмите на кнопку **+ Прошивка**.

4. Укажите путь к архиву с прошивкой. При указании пути вы можете выбрать несколько архивов одновременно.

Прошивка будет загружена и отобразится в таблице.

Запланированное обновление прошивки на выбранных устройствах CPE

Чтобы создать задачу по запланированному обновлению прошивки на выбранных устройствах CPE:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Перейдите к запланированному обновлению прошивки одним из следующих способов:

   - Если вы хотите выполнить запланированное обновление прошивки на отдельном устройстве CPE, нажмите на устройство CPE, в открывшемся окне свойств устройства вызовите меню действий, нажав на значок ⋮ в правом верхнем углу, и выберите пункт **Обновить прошивку**.

   - Если вы хотите выполнить запланированное обновление прошивки на нескольких устройствах CPE, установите флажки рядом с устройствами CPE и в верхней части таблицы нажмите на кнопку **Действия** → **Обновить прошивку**.

   Устаревшие прошивки подсвечиваются оранжевым цветом в столбце **Версия ПО** таблицы устройств CPE. Вы также можете найти устройства CPE с устаревшими версиями прошивок с помощью фильтра **Необходимо обновление**, который отображается в верхней части таблицы.

3. В открывшемся окне в поле **Имя задачи** введите имя запланированной задачи.

4. С помощью переключателя **Тип коммутатора** выберите тип программного коммутатора для новой прошивки (OVS или SWOS).

   Если вы обновляете прошивку на нескольких устройствах CPE одновременно, необходимо выбрать тип программного коммутатора, которому соответствуют прошивки всех выбранных устройства. Если тип прошивки хотя бы на одном устройстве не соответствует выбранному типу программного коммутатора, то в окне создания задачи обновления прошивки появится сообщение **Обновить CPE можно только на прошивку с тем же типом коммутатора**, и создание задачи будет невозможным. Если вы обновляете прошивку на одном устройстве, то при выборе отличающегося типа коммутатора появится предупреждение **Выбранный тип коммутатора не соответствует типу коммутатора CPE. После обновления прошивки устройство может стать недоступным из-за потенциальной несовместимости параметров**, но создание задачи будет возможным.

   Обновление прошивки на версию, основанную на другом типе программного коммутатора, не рекомендуется.

5. В раскрывающемся списке **Версия** выберите версию загруженной прошивки. В списке отображаются версии прошивок, соответствующие типу программного коммутатора, выбранному в параметре **Тип коммутатора**. Если вы не знаете, какую версию прошивки требуется установить на устройстве CPE, используйте таблицу соответствия моделей устройств CPE версиям прошивок.

   Если в списке отсутствуют подходящие версии прошивок (не найдены версии, соответствующие выбранному типу программного коммутатора, либо в оркестратор не были загружены никакие версии), то в верхней части окна появится сообщение **Для выбранных CPE нет доступных прошивок. Вы можете загрузить новые прошивки** со ссылкой на раздел **SD-WAN → Прошивка**.

6. В поле **Запланированное время выполнения задачи** введите дату и время выполнения задачи. По умолчанию указана дата и время в момент, когда вы начали создавать задачу.

7. Если вы хотите сбросить параметры устройства CPE до заводских значений после обновления прошивки, снимите флажок **Сохранить параметры CPE**. Когда флажок установлен, после обновления прошивки параметры устройства CPE остаются без изменений. Этот флажок установлен по умолчанию.

   При сбросе параметров до заводских значений устройство CPE отключается от оркестратора. Для повторного подключения устройства CPE к оркестратору вам нужно автоматически зарегистрировать устройство CPE (ZTP).

8. При необходимости обновить прошивку принудительно, даже если внутренняя проверка на устройстве CPE выявляет несовместимость его текущей прошивки с новой, установите флажок **Принудительное обновление**. Этот флажок снят по умолчанию.

9. Нажмите на кнопку **Далее**.

   Отобразятся две таблицы устройств CPE. Прошивка устройств CPE из верхней таблицы будет обновлена. Прошивка устройств CPE из нижней таблицы не будет обновлена. Информация об устройствах CPE отображается в следующих столбцах таблицы:

   - **DPID** – идентификатор DPID устройства CPE.
   - **Модель** – модель устройства CPE.
   - **Тип коммутатора** – тип программного коммутатора прошивки устройства CPE (OVS или SWOS).
   - **Имя** – имя устройства CPE.
   - **Версия ПО** – версия прошивки устройства CPE.
   - **Тенант** – тенант, которому было добавлено устройство CPE.
   - **Причина** – причина, по которой прошивку невозможно обновить. Этот столбец отображается только в нижней таблице.

   Если в верхнюю таблицу попали устройства CPE, на которых вы не хотите обновлять прошивку, вы можете перенести эти устройства CPE в нижнюю таблицу.

10. Нажмите на кнопку **Запланировать**.

    Задача по обновлению прошивки будет создана и отобразится в таблице задач. Статус задач отображается в столбце **Статус**. При успешном выполнении задачи по обновлению прошивки ее статус изменяется на **Выполнено**.

Запланированное обновление прошивки на устройствах CPE с указанными тегами

Чтобы создать задачу по запланированному обновлению прошивки на устройствах CPE с указанными тегами:

1. В меню перейдите в раздел **Планировщик**.

   Отобразится таблица задач.

2. В верхней части страницы нажмите на кнопку **+ Задача**.

3. В открывшемся окне в раскрывающемся списке **Тип** выберите **Обновление прошивки**.

4. В поле **Имя задачи** введите имя задачи.

5. С помощью переключателя **Тип коммутатора** выберите тип программного коммутатора для новой прошивки (OVS или SWOS).

6. В раскрывающемся списке **Версия** выберите версию загруженной прошивки. В списке отображаются версии прошивок, соответствующие типу программного коммутатора, выбранному в параметре **Тип коммутатора**. Если вы не знаете, какую версию прошивки требуется установить на устройстве CPE, используйте таблицу соответствия моделей устройств CPE версиям прошивок.

   Если в списке отсутствуют подходящие версии прошивок (не найдены версии, соответствующие выбранному типу программного коммутатора, либо в оркестратор не были загружены никакие версии), то в верхней части окна появится сообщение **Для выбранных CPE нет доступных прошивок. Вы можете загрузить новые прошивки** со ссылкой на раздел **SD-WAN → Прошивка**.

7. В поле **Запланированное время выполнения задачи** введите дату и время выполнения задачи. По умолчанию указана дата и время в момент, когда вы начали создавать задачу.

8. Если вы хотите сбросить параметры устройства CPE до заводских значений после обновления прошивки, снимите флажок **Сохранить параметры CPE**. Когда флажок установлен, после обновления прошивки параметры устройства CPE остаются без изменений. Этот флажок установлен по умолчанию.

   При сбросе параметров до заводских значений устройство CPE отключается от оркестратора. Для повторного подключения устройства CPE к оркестратору вам нужно автоматически зарегистрировать устройство CPE (ZTP).

9. При необходимости обновить прошивку принудительно, даже если внутренняя проверка на устройстве CPE выявляет несовместимость его текущей прошивки с новой, установите флажок **Принудительное обновление**. Этот флажок снят по умолчанию.

10. В поле **Теги** введите теги, назначенные устройствам CPE, на которых вы хотите обновить прошивку. Устаревшие прошивки подсвечиваются оранжевым цветом в столбце **Версия ПО** таблицы устройств CPE. Вы также можете найти устройства CPE с устаревшими версиями прошивок с помощью фильтра **Необходимо обновление**, который отображается в верхней части таблицы.

11. Нажмите на кнопку **Далее**.

    Отобразятся две таблицы устройств CPE. Прошивка устройств CPE из верхней таблицы будет обновлена. Прошивка устройств CPE из нижней таблицы не будет обновлена. Информация об устройствах CPE отображается в следующих столбцах таблицы:

    - **DPID** – идентификатор DPID устройства CPE.
    - **Модель** – модель устройства CPE.
    - **Тип коммутатора** – тип программного коммутатора прошивки устройства CPE (OVS или SWOS).
    - **Имя** – имя устройства CPE.
    - **Версия ПО** – версия прошивки устройства CPE.
    - **Тенант** – тенант, которому было добавлено устройство CPE.
    - **Причина** – причина, по которой прошивку невозможно обновить. Этот столбец отображается только в нижней таблице.

    Если в верхнюю таблицу попали устройства CPE, на которых вы не хотите обновлять прошивку, вы можете перенести эти устройства CPE в нижнюю таблицу.

12. Нажмите на кнопку **Создать**.

Задача по обновлению прошивки будет создана и отобразится в таблице. Статус задач отображается в столбце **Статус**. При успешном выполнении задачи по обновлению прошивки ее статус изменяется на **Выполнено**.

Восстановление прошивки устройства CPE модели KESR-M1

Вы можете восстановить прошивку и сбросить параметры устройства CPE модели KESR-M1 до заводских значений, если вы утратили учетные данные устройства CPE, или при неисправности прошивки.

При сбросе параметров до заводских значений устройство CPE отключается от оркестратора. Для повторного подключения устройства CPE к оркестратору вам нужно автоматически зарегистрировать устройство CPE (ZTP).

Чтобы восстановить прошивку устройства CPE модели KESR-M1:

1. Скачайте архив с прошивкой из директории /cpe комплекта поставки на устройство администратора, например на ноутбук. Если вы не знаете, какую версию прошивки требуется установить на устройстве CPE, используйте таблицу соответствия моделей устройств CPE версиям прошивок.

2. Распакуйте архив с прошивкой, чтобы получить прошивку в формате BIN.

3. Включите устройство CPE с заводской прошивкой:

   a. Отключите кабель питания устройства CPE.

   b. Подключите кабель питания и удерживайте кнопку **RESET** на устройстве CPE в течение 10 секунд.

   Устройство CPE включится с заводской прошивкой.

4. Подключите устройство администратора к LAN-порту устройства CPE.

   Устройство администратора получит IP-адрес и IP-адрес шлюза по умолчанию из подсети 192.168.1.0/24 по протоколу DHCP.

5. В адресной строке браузера на устройстве администратора введите `192.168.1.1` и нажмите на клавишу **Enter**.

   Откроется страница загрузки прошивки устройства CPE.

6. Нажмите на кнопку загрузки прошивки и укажите путь к прошивке в формате BIN. Вы получили прошивку в формате BIN на шаге 2 этой инструкции.

На устройстве CPE будет установлена новая версия прошивки, после чего устройство CPE перезагрузится. По умолчанию IP-адрес устройства CPE – 192.168.7.1, и на LAN-портах включен протокол DHCP.

Восстановление прошивки устройства CPE модели KESR-M2–5

Вы можете восстановить прошивку и сбросить параметры устройства CPE модели KESR-M2–5 до заводских значений, если вы утратили учетные данные устройства CPE, или при неисправности прошивки.

При сбросе параметров до заводских значений устройство CPE отключается от оркестратора. Для повторного подключения устройства CPE к оркестратору вам нужно автоматически зарегистрировать устройство CPE (ZTP).

Чтобы восстановить прошивку устройства CPE модели KESR-M2–5:

1. Скачайте архив с прошивкой из директории /cpe комплекта поставки на устройство администратора, например на ноутбук. Если вы не знаете, какую версию прошивки требуется установить на устройстве CPE, используйте таблицу соответствия моделей устройств CPE версиям прошивок.

2. Распакуйте архив с прошивкой, чтобы получить архив в формате IMG.GZ.

3. Распакуйте архив в формате IMG.GZ, чтобы получить образ прошивки в формате IMG.

4. Создайте загрузочный диск из прошивки в формате IMG на USB-накопителе с помощью программы для записи образов дисков, например BalenaEtcher.

5. Подключите устройство администратора к устройству CPE с помощью консольного кабеля и вставьте USB-накопитель в USB-порт устройства CPE.

6. Укажите параметры установки консольной сессии с устройством CPE на устройстве администратора, например с помощью программы PuTTY, при этом выполнив следующие действия:

   - Укажите номер последовательного порта (англ. communications port, COM port) устройства администратора.

   - Укажите значение `115200` для скорости сессии.

7. Отключите и подключите кабель питания устройства CPE. При включении устройства CPE нажмите на клавишу **F7** или **F11**.

8. В открывшемся меню выберите USB-накопитель и нажмите на клавишу **Enter**.

   Устройство CPE загрузится с USB-накопителя.

9. Подключите устройство администратора к LAN-порту устройства CPE.

   Устройство администратора получит IP-адрес и IP-адрес шлюза по умолчанию из подсети 192.168.7.0/24 по протоколу DHCP.

10. Подключитесь к устройству CPE по протоколу SCP, например с помощью программы WinSCP. Для подключения по протоколу SCP вам нужно указать IP-адрес и ввести учетные данные по умолчанию устройства CPE.

11. Поместите прошивку в формате IMG в директорию /tmp.

12. Подключитесь к устройству CPE по протоколу SSH или установите с устройством CPE консольную сессию. Для подключения по протоколу SSH или установки консольной сессии вам нужно указать IP-адрес и ввести учетные данные по умолчанию устройства CPE.

13. Перейдите в директорию /tmp, выполнив команду:

    ```
    cd /tmp/
    ```

14. Скопируйте образ прошивки в формате IMG в директорию /dev/sda, выполнив команду:

    ```
    dd if=< имя файла прошивки в формате IMG > bs=1M of=/dev/sda
    ```

15. Перезагрузите устройство CPE, выполнив команду:

    ```
    reboot
    ```

    На устройстве CPE будет установлена новая версия прошивки, после чего устройство CPE перезагрузится. По умолчанию IP-адрес устройства CPE – 192.168.7.1, и на LAN-портах включен протокол DHCP.

Соответствие моделей устройств CPE версиям прошивок

В таблице ниже приведено соответствие между моделями устройств CPE и поддерживаемыми версиями прошивок.

Модель устройства CPE	KESR M1
KESR M1 (V1 TTK)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.firmware.kesr-m1-r-5g-1l-w-v1-ttk_en-US_ru-RU.tar.gz
KESR M1 (V2)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.firmware.kesr-m1-r-5g-2l-w-v2_en-US_ru-RU.tar.gz
KESR M1 (V3)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.efi.amd64-kesr-m1-k-4g-2l-w-v3_en-US_ru-RU.tar.gz
KESR M2 (Wi-Fi/LTE)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.efi.amd64-kesr-m2-k-5g-1l-w_en-US_ru-RU.tar.gz
KESR M2 (SFP)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.efi.amd64-kesr-m2-k-5g-1s_en-US_ru-RU.tar.gz
KESR M3	knaas-cpe_<версия прошивки>.release.<номер версии решения>.efi.amd64-kesr-m3-k-4g-4s_en-US_ru-RU.tar.gz
KESR M4 (SFPx2)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.efi.amd64-kesr-m4-k-4g-2x_en-US_ru-RU.tar.gz
KESR M4 (SFPx4/RJ-45x8)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.efi.amd64-kesr-m4-k-8g-4x_en-US_ru-RU.tar.gz
KESR M5 (SFPx8)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.efi.amd64-kesr-m5-k-4g-8x_en-US_ru-RU.tar.gz
KESR M5 (SFPx4/RJ-45x8)	knaas-cpe_<версия прошивки>.release.<номер версии решения>.efi.amd64-kesr-m5-k-8g-4x_en-US_ru-RU.tar.gz

Удаление прошивки

Вы не можете удалить прошивку, которая используется хотя бы в одной задаче. Для удаления прошивки, которая используется в задачах, вам нужно сначала удалить задачи.

Удаленные прошивки невозможно восстановить.

Чтобы удалить прошивку:

1. В меню перейдите в раздел **SD-WAN → Прошивка**.

   Отобразится таблица прошивок.

2. Установите флажки рядом с прошивками, которые вы хотите удалить.

3. В верхней части таблицы нажмите на кнопку **Действия → Удалить**.

4. В окне подтверждения нажмите на кнопку **Удалить**.

Прошивки будут удалены и перестанут отображаться в таблице.

Дополнительная настройка устройств CPE с помощью скриптов

Для дополнительной настройки устройств CPE используются скрипты. Вы можете добавить скрипты в шаблон CPE. Скрипты, добавленные в шаблон CPE, автоматически добавляются на всех устройствах CPE, которые используют шаблон CPE. Добавленные скрипты запускаются автоматически или вручную. Автоматический запуск скриптов происходит при соблюдении указанных в параметрах скрипта условий, например при регистрации устройства CPE.

Запуск скриптов обеспечивает VNFM, поэтому перед началом работы со скриптами необходимо обеспечить сетевую связность между VNFM и устройствами CPE. По умолчанию в шаблоне CPE указан номер порта для подключения VNFM к устройству и имя учетной записи для запуска скриптов. При необходимости вы можете изменить номер порта и имя учетной записи.

Вы можете посмотреть таблицу скриптов в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы скриптов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **Скрипты**.
- Для просмотра таблицы скриптов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Скрипты**.

Информация о скриптах отображается в следующих столбцах таблицы:

- **Имя** – имя скрипта.
- **Интерпретатор** – интерпретатор.
- **Аутентификация** – тип аутентификации VNFM в устройстве CPE.
- **Пользовательский интерпретатор** – путь к пользовательскому интерпретатору.
- **Время (сек.)** – время в секундах, по прошествии которого VNFM перестает предпринимать попытки запуска скрипта, который не запустился с первого раза.

- **Повторный запуск** – скрипт может быть повторно запущен:
  - **Да**.
  - **Нет**.
- **Стадия** – стадия работы устройства CPE, на которой VNFM запускает скрипт.
- **Скрипт** – имя файла со скриптом или файла-сценария Ansible playbook.
- **Файл** – имя архива с дополнительными файлами, необходимыми для запуска скрипта.
- **Действия** – действия, которые можно выполнить со скриптом.

Добавление скрипта на устройства CPE

Вы можете добавить скрипт в шаблон CPE. Скрипты, добавленные в шаблон CPE, автоматически добавляются на все устройства CPE, которые используют шаблон CPE.

Чтобы добавить скрипт на устройства CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, в который вы хотите добавить скрипт.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, имя учетной записи для запуска скриптов и таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **+ Скрипт**.

5. В открывшемся окне в поле **Имя** введите имя скрипта. Максимальная длина имени: 255 символов.

6. В поле **Время (сек.)** введите время в секундах, по прошествии которого VNFM перестает предпринимать попытки запуска скрипта, который не запустился с первого раза. Значение по умолчанию: `360`.

7. В раскрывающемся списке **Интерпретатор** выберите одно из следующих значений:
   - **Ansible**. Это значение выбрано по умолчанию.
   - **Shell**.
   - **Expect**.
   - **Пользовательский** – использовать интерпретатор на устройстве CPE. При выборе этого значения в поле **Пользовательский интерпретатор** введите путь к пользовательскому интерпретатору.

8. В раскрывающемся списке **Стадия** выберите, на какой стадии работы устройства CPE VNFM запускает скрипт:

   - **Регистрация**. Это значение выбрано по умолчанию.
   - **Удаление**.
   - **Вручную** – запускать скрипт только вручную.

9. При необходимости повторно запускать скрипт установите флажок **Повторный запуск**. Этот флажок снят по умолчанию. Существуют следующие особенности повторного запуска:

   - Если в раскрывающемся списке **Стадия** вы выбрали **Регистрация**, скрипт повторно запускается при регистрации, включении питания и перезагрузке устройства CPE.
   - Если в раскрывающемся списке **Стадия** вы выбрали **Удаление**, скрипт не запускается повторно.
   - Если в раскрывающемся списке **Стадия** вы выбрали **Вручную**, скрипт повторно запускается при включении питания и перезагрузке устройства CPE.

10. В поле **Скрипт** укажите путь к файлу со скриптом или к файлу-сценарию Ansible playbook.

11. При необходимости в поле **Файл** укажите путь к архиву с дополнительными файлами, необходимыми для запуска скрипта. Поддерживаемые форматы архивов с файлами: TAR.GZ и ZIP.

12. Нажмите на кнопку **Сохранить**.

    Скрипт будет добавлен и отобразится в таблице.

13. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE.

Запуск скриптов вручную на устройствах CPE

Вы можете вручную запустить отдельный скрипт или все скрипты в шаблоне CPE или на устройстве CPE. Скрипты, запущенные в шаблоне CPE, автоматически запускаются на всех устройствах CPE, которые используют шаблон CPE, или на устройствах CPE с указанными тегами.

Запуск скриптов вручную в шаблоне CPE

Чтобы вручную запустить скрипты в шаблоне CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, в котором вы хотите вручную запустить скрипты.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, имя учетной записи для запуска скриптов и таблица скриптов, если добавлен хотя бы один скрипт.

4. Если вы хотите вручную запустить отдельный скрипт, выполните следующие действия:

   a. Нажмите на кнопку **Запустить** рядом со скриптом, который вы хотите запустить вручную.

   b. В открывшемся окне выберите, на каких устройствах CPE запускается скрипт:

   - **Запустить скрипт <имя скрипта> на всех связанных CPE** – запустить скрипт на всех устройствах CPE, которые используют шаблон CPE. Это значение выбрано по умолчанию.
   - **Запустить скрипт <имя скрипта> на всех связанных CPE с тегами** – запустить скрипт на устройствах CPE с указанными тегами, которые используют шаблон CPE. При выборе этого значения в нижней части окна укажите теги.

5. Если вы хотите вручную запустить все скрипты, выполните следующие действия:

   a. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Запустить скрипты**.

   b. В открывшемся окне выберите, на каких устройствах CPE запускаются скрипты:

   - **Запустить скрипты на всех связанных CPE** – запустить скрипты на всех устройствах CPE, которые используют шаблон CPE. Это значение выбрано по умолчанию.
   - **Запустить скрипты на всех связанных CPE с тегами** – запустить скрипты на устройствах CPE с указанными тегами, которые используют шаблон CPE. При выборе этого значения в нижней части окна укажите теги.

6. Нажмите на кнопку **Запустить**.

Скрипты будут запущены.

Запуск скриптов вручную на устройстве CPE

Чтобы вручную запустить скрипты на устройстве CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, в котором вы хотите вручную запустить скрипты.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, имя учетной записи для запуска скриптов и таблица скриптов, если добавлен хотя бы один скрипт.

4. Запустите скрипты вручную одним из следующих способов:

   - Если вы хотите вручную запустить отдельный скрипт, нажмите на кнопку **Запустить** рядом с этим скриптом.

   - Если вы хотите вручную запустить все скрипты, в верхней части области настройки в блоке **Действия** нажмите на кнопку **Запустить скрипты**.

5. В открывшемся окне нажмите на кнопку **Запустить**.

Скрипты будут запущены.

Запланированный запуск скриптов на устройствах CPE

Задачи по запланированному запуску скриптов на устройствах CPE можно создать в планировщике задач. При создании задачи необходимо выбрать шаблон CPE, скрипты, а также устройства CPE, на которых скрипты будут запущены.

Вы можете запустить скрипты на всех устройствах CPE, которые используют шаблон CPE, или ограничить количество устройств CPE, указав теги или выбрав устройства CPE вручную.

Чтобы создать задачу по запуску скриптов на устройствах CPE:

1. В меню перейдите в раздел **Планировщик**.

   Отобразится таблица запланированных задач.

2. В верхней части страницы нажмите на кнопку **+ Задача**.

3. В открывшемся окне в раскрывающемся списке **Тип** выберите **Запуск скрипта**.

4. В поле **Имя** введите имя задачи.

5. В раскрывающемся списке **CPE для запуска скрипта** выберите, на каких устройствах CPE запускаются скрипты:

   - **Все CPE с выбранным шаблоном** – запустить скрипты на всех устройствах CPE, которые используют шаблон CPE.

   - **Все CPE с выбранным шаблоном и определенными тегами** – запустить скрипты на устройствах CPE с указанными тегами, которые используют шаблон CPE. При выборе этого значения в поле **Теги** укажите теги устройств CPE.

   - **Определенные CPE с выбранным шаблоном** – запустить скрипты на выбранных вручную устройствах CPE, которые используют шаблон CPE. При выборе этого значения в блоке **[[scheduler.fields.cpes]]** выберите устройства CPE.

6. В блоке **Шаблон CPE** выберите шаблон CPE, содержащий скрипты, которые вы хотите запустить.

7. В блоке **Скрипты** выберите скрипты, которые вы хотите запустить.

8. В поле **Запланированное время выполнения задачи** введите дату и время выполнения задачи. По умолчанию указаны дата и время в момент, когда вы начали создавать задачу.

9. Нажмите на кнопку **Создать**.

Задача по запланированному запуску скрипта будет создана и отобразится в таблице. Статус задач отображается в столбце **Статус**. При успешном выполнении задачи по запуску скрипта ее статус изменяется на **Выполнено**.

Изменение скрипта на устройствах CPE

Вы можете изменить скрипт в шаблоне CPE. Скрипт, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить скрипт на устройствах CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, в котором вы хотите изменить скрипт.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, имя учетной записи для запуска скриптов и таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **Изменить** рядом со скриптом, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры скрипта. Описание параметров см. в инструкции по добавлению скрипта на устройствах CPE.

6. Нажмите на кнопку **Сохранить**.

   Скрипт будет изменен и обновится в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE.

Удаление скрипта на устройствах CPE

Вы можете удалить скрипт в шаблоне CPE. Скрипт, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE.

Удаленные скрипты невозможно восстановить.

Чтобы удалить скрипт на устройствах CPE:

1. В меню перейдите в подраздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, имя учетной записи для запуска скриптов и таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **Удалить** рядом со скриптом, который вы хотите удалить.

   Скрипт будет удален и перестанет отображаться в таблице.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE.

Настройка параметров DNS на устройствах CPE

Включение DNS на сетевых интерфейсах

По умолчанию DNS-серверы, указанные при создании сетевых интерфейсов или в правилах условной переадресации DNS, не активны ни на одном интерфейсе. Чтобы устройство CPE обрабатывало DNS-запросы, вам необходимо включить использование DNS на нужных интерфейсах в шаблоне CPE или на устройстве CPE.

Чтобы включить использование DNS:

1. Перейдите к включению использования DNS одним из следующих способов:

   - Если вы хотите включить использование DNS на интерфейсах в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE** и нажмите на нужный шаблон CPE.

   - Если вы хотите включить использование DNS на интерфейсах устройства CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на нужное устройство CPE.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

2. В меню слева выберите раздел **DNS** и перейдите на вкладку **Интерфейсы DNS**.

   Отобразится таблица **Включение/выключение DNS-сервера на интерфейсах**.

   В таблице отсутствуют интерфейсы, которые используются в виртуальных таблицах маршрутизации. Такие интерфейсы не поддерживаются устройствами CPE для обработки DNS-запросов.

3. Включите переключатель в столбце **Включено** для интерфейсов, на которых вы хотите включить обработку DNS-запросов.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Использование DNS на интерфейсах будет включено, и устройство CPE будет использовать указанные при создании сетевых интерфейсов или в правилах условной переадресации DNS-серверы при обработке DNS-запросов.

Работа с правилами условной переадресации DNS

Вы можете настроить на устройстве CPE условную переадресацию DNS, чтобы перенаправлять полученные на CPE DNS-запросы на вышестоящие DNS-серверы в зависимости от суффикса имени, указанного в DNS-запросе (например, чтобы блокировать доступ к нежелательным ресурсам или направлять запросы к корпоративным ресурсам на внутренние DNS-серверы).

Для использования условной переадресации DNS вам необходимо настроить правила переадресации, по которым будут обрабатываться DNS-запросы для выбора нужного DNS-сервера в зависимости от указанного в правиле суффикса.

Условная переадресация DNS не совместима с использованием виртуальных таблиц маршрутизации: интерфейсы, используемые в экземпляре VRF, не могут использоваться устройством CPE для обработки DNS-запросов.

Создание правил условной переадресации

Вы можете создать правила условной переадресации в шаблоне CPE или на устройстве CPE. Правила, созданные в шаблоне CPE, автоматически создаются на всех устройствах CPE, которые используют шаблон CPE.

По умолчанию DNS-серверы не активны ни на одном интерфейсе. Чтобы устройство CPE обрабатывало DNS-запросы, вам необходимо включить использование DNS на нужных интерфейсах.

Чтобы создать правило условной переадресации:

1. Перейдите к созданию правила условной переадресации одним из следующих способов:

   - Если вы хотите создать правило условной переадресации в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE** и нажмите на нужный шаблон CPE.

   - Если вы хотите создать правило условной переадресации на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE** и нажмите на нужное устройство CPE.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

2. В меню слева выберите раздел **DNS** и перейдите на вкладку **Условная переадресация DNS**.

   Отобразится таблица правил условной переадресации.

3. В верхней части таблицы нажмите на кнопку **+ Создать**.

4. В открывшемся окне задайте нужные параметры правила переадресации:

   a. Включите переключатель **Включено**, если хотите, чтобы созданное правило использовалось на устройстве CPE. Оставьте переключатель выключенным, если хотите создать правило, но не использовать его на устройстве CPE.

   b. В поле **Суффикс** укажите суффикс, по которому DNS-запросы должны перенаправляться на DNS-сервер с указанным IP-адресом.

   Суффикс должен быть уникальным для каждого правила. Максимальная длина – 255 символов. Значение поля представляет собой строку вида:

   ```
   <label1>[.<label>]
   ```

   (элемент `<label1>,` за которым следует необязательный набор элементов `<label>`, разделенных точкой), где `<label>` – подстрока из допустимых символов `[a-zA-Z0-9-]` длиной от 1 до 63 символов, `<label1>` – подстрока из тех же допустимых символов с опциональным символом подстановки `*` в начале.

   Если в суффиксе есть один или более `<label>` после `<label1>`, то `<label1>` может состоять из единственного символа *, если же в суффиксе нет ни одного одного `<label>`, то в `<label1>` после символа * всегда должны следовать другие символы из допустимых.

   Примеры:

   Допустимые значения:

   *.example.com

   *example.com

   Недопустимые значения:

   *

   www.*.com

   www.*example.com

   c. Добавьте один или несколько вышестоящих DNS-серверов, на которые должны перенаправляться DNS-запросы:

   - В поле **Вышестоящий DNS** укажите IP-адрес DNS-сервера, которому должны перенаправляться DNS-запросы при совпадении с суффиксом этого правила.
   - В списке **Псевдоним** выберите псевдоним интерфейса, с которого должны отправляться DNS-запросы в рамках этого правила.

   При необходимости нажмите на кнопку **Добавить вышестоящий DNS**, чтобы добавить следующий вышестоящий DNS-сервер. Вы можете добавить максимум 15 вышестоящих DNS-серверов для одного суффикса

5. Нажмите на кнопку **Сохранить**.

   Правило условной переадресации будет создано и отобразится в таблице.

6.

7. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение правил условной переадресации

Вы можете изменить правила условной переадресации в шаблоне CPE или на устройстве CPE. Правила, измененные в шаблоне CPE, автоматически изменяются на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить правило условной переадресации:

1. Перейдите к изменению правила условной переадресации одним из следующих способов:

   - Если вы хотите изменить правило условной переадресации в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE** и нажмите на шаблон CPE, на котором вы хотите изменить правило переадресации.

   - Если вы хотите изменить правило условной переадресации на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, на котором вы хотите изменить правило переадресации.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

2. В меню слева выберите раздел **DNS** и перейдите на вкладку **Условная переадресация DNS**.

   Отобразится таблица правил условной переадресации.

3. Выберите правило условной переадресации, которое вы хотите изменить, и нажмите на кнопку **Изменить**.

4. В открывшемся окне измените нужные параметры правила переадресации. Описание параметров см. в статье Создание правил условной переадресации.

5. Нажмите на кнопку **Сохранить**.

   Правило условной переадресации будет изменено и обновится в таблице.

6. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление правил условной переадресации

Чтобы удалить правила условной переадресации:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите удалить правила.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В меню слева выберите раздел **DNS** и перейдите на вкладку **Условная переадресация DNS**.

   Отобразится таблица правил условной переадресации.

4. Выберите одно или несколько правил условной переадресации, которые вы хотите удалить, и нажмите на кнопку **Удалить**.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Правила условной переадресации будут удалены и перестанут отображаться в таблице.

Настройка подключения устройства CPE к оркестратору и контроллеру

При регистрации устройство CPE подключается к оркестратору и контроллеру. Вы можете указать параметры подключения устройства CPE к оркестратору и контроллеру в шаблоне CPE или на устройстве CPE. Параметры подключения устройства CPE к оркестратору и контроллеру, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

На некоторых моделях аппаратных CPE размещены дополнительные LED-индикаторы, которые отображают состояние соединения с контроллером, соединения с оркестратором, а также, если на устройстве включена функция CPE, наличие активных туннелей. Более подробную информацию о работе LED-индикаторов можно получить из документации к устройствам или обратившись в Службу технической поддержки.

Чтобы настроить подключение устройства CPE к оркестратору и контроллеру:

1. Перейдите к настройке подключения устройства CPE к оркестратору и контроллеру одним из следующих способов:

   - Если вы хотите настроить подключение к оркестратору и контроллеру в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **SD-WAN → Основные параметры**.

   - Если вы хотите настроить подключение к оркестратору и контроллеру на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите устройство CPE, выберите вкладку **SD-WAN → Основные параметры** и установите флажок **Переопределить**.

   Отобразятся параметры подключения устройства CPE к оркестратору и контроллеру.

2. В блоке **Подключение к оркестратору** укажите параметры подключения устройства CPE к оркестратору:

   a. В поле **IP/FQDN оркестратора** введите IP-адрес или FQDN оркестратора. Максимальная длина FQDN: 50 символов.

   b. В поле **Порт оркестратора** введите номер порта оркестратора. Диапазон значений: от 0 до 65 535.

   c. Если вы хотите, чтобы устройство CPE получало номер порта оркестратора по протоколу DNS, включите переключатель **Получить порт оркестратора через DNS**. Для использования этой функции предварительно необходимо создать на DNS-сервере TXT-запись, хранящую нужный номер порта, в формате `_port.<FQDN>`, где `<FQDN>` – указанный в поле поле **IP/FQDN оркестратора** адрес оркестратора.

   d. Если вы хотите использовать резервный оркестратор при выходе из строя основного оркестратора, в блоке **IP-адрес и порт резервного оркестратора** выполните следующие действия:

      1. Установите флажок **Включено**. Этот флажок снят по умолчанию.

      2. В поле **IP/FQDN резервного оркестратора** введите IP-адрес или FQDN резервного оркестратора. Максимальная длина FQDN: 50 символов.

      3. В поле **Порт резервного оркестратора** введите номер порта резервного оркестратора. Диапазон значений: от 0 до 65 535.

   e. В раскрывающемся списке **Протокол оркестратора** выберите протокол подключения устройства CPE к оркестратору:

      - **http**;

      - **https**. Это значение выбрано по умолчанию.

      Этот параметр можно указать только в шаблоне CPE.

   f. В поле **Интервал обновления (сек.)** введите интервал времени в секундах для отправки устройством CPE REST API-запросов оркестратору. Диапазон значений: от 5 до 300. Значение по умолчанию: `30`.

   g. В поле **Интервал интерактивного режима (сек.)** введите интервал времени в секундах для отправки устройством CPE REST API-запросов оркестратору в интерактивном режиме. Диапазон значений: от 1 до 10. Вы можете включить интерактивный режим для диагностики устройства CPE.

h. В поле **Таймаут интерактивного режима (сек.)** введите время в секундах, по прошествии которого на устройстве CPE выключается интерактивный режим. Диапазон значений: от 30 до 180.

3. В блоке **Подключение к контроллеру** укажите параметры подключения устройства CPE к контроллеру:

   a. В раскрывающемся списке **OpenFlow-транспорт** укажите, шифруются ли управляющие сессии между интерфейсами SD-WAN с типом WAN устройства CPE и узлами контроллера:

      - **TCP** – не шифровать управляющие сессии.
      - **SSL** – шифровать управляющие сессии. Это значение выбрано по умолчанию.

      Этот параметр можно указать только в шаблоне CPE.

   b. В раскрывающемся списке **Интерфейс SD-WAN управления** выберите, с какого интерфейса SD-WAN с типом WAN в приоритете устанавливается основная управляющая сессия:

      - **Случайно** – основная управляющая сессия устанавливается со случайно выбранного интерфейса SD-WAN с типом WAN. Это значение выбрано по умолчанию.
      - **<интерфейс SD-WAN с типом WAN>** – основная управляющая сессия устанавливается с указанного интерфейса SD-WAN с типом WAN. Если указанный интерфейс SD-WAN с типом WAN недоступен, основная управляющая сессия устанавливается со случайно выбранного интерфейса SD-WAN с типом WAN.

      При выходе из строя интерфейса SD-WAN с типом WAN, с которого установлена основная управляющая сессия, новая основная управляющая сессия выбирается случайно из ранее установленных управляющих сессий. Если в раскрывающемся списке **Интерфейс SD-WAN управления** вы выбрали **<интерфейс SD-WAN с типом WAN>** и вы хотите, чтобы управляющая сессия, установленная с указанного интерфейса SD-WAN с типом WAN, снова становилась основной при восстановлении интерфейса SD-WAN с типом WAN, выполните следующие действия:

      1. Установите флажок **Preemption**. Этот флажок снят по умолчанию.
      2. В поле **Время** введите время в секундах, по прошествии которого управляющая сессия, установленная с указанного интерфейса SD-WAN с типом WAN, снова становится основной при восстановлении интерфейса SD-WAN с типом WAN. Диапазон значений: от 0 до 86 400.

   c. В раскрывающемся списке **Автоперезагрузка** выберите, перезагружается ли устройство CPE при длительном разрыве управляющих сессий с узлами контроллера:

      - **Да**. При выборе этого значения в поле **Время перезагрузки (сек.)** введите время в секундах, по прошествии которого устройство CPE перезагружается при разрыве управляющих сессий с узлами контроллера. Диапазон значений: от 60 до 2 073 600.
      - **Нет**. Это значение выбрано по умолчанию.

   d. В поле **Конфигурационный URL** введите шаблон веб-адреса базовыми параметрами устройства CPE. При вводе шаблона учитывайте следующие ограничения:

      - `{config}` – обязательная часть, которая при генерации ссылки из шаблона заменяется на параметры устройства CPE.
      - Максимальная длина: 128 символов.
      - Требуется указать `http` или `https`.

      По умолчанию используется шаблон `http://192.168.7.1/cgi-bin/config?payload={config}`.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Настройка параметров подключения к устройству CPE через системную консоль

Вы можете устанавливать консольную сессию с устройством CPE, например, для восстановления прошивки или диагностики устройства. Модели M2 и старше оснащены внешним последовательным портом для подключения к системной консоли. Для модели M1 подключение к системной консоли осуществляется с помощью переходника через разъем UART, находящийся под крышкой устройства.

После получения доступа к системной консоли вам потребуется указать учетные данные для входа в систему. Вы можете настроить аутентификацию на системной консоли через веб-интерфейс оркестратора в шаблоне CPE или на устройстве CPE.

Чтобы настроить аутентификацию на системной консоли:

1. Перейдите к настройке аутентификации на системной консоли одним из следующих способов:

   - Если вы хотите настроить аутентификацию на системной консоли в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **SD-WAN → Основные параметры**.

   - Если вы хотите настроить подключение к системной консоли на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите устройство CPE, выберите вкладку **SD-WAN → Основные параметры** и установите флажок **Переопределить**.

   Отобразятся параметры подключений устройства CPE.

2. В блоке **Параметры консоли** включите переключатель **Аутентификация на системной консоли**, чтобы при подключении через системную консоль запрашивались учетные данные пользователя, или выключите его, чтобы учетные данные не запрашивались. По умолчанию переключатель выключен.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение вступит в силу только после того, как вы перезагрузите устройство вручную.

Работа с сетевыми интерфейсами

Сетевые интерфейсы соответствуют портам и виртуальным интерфейсам операционной системы устройства CPE, которые подключаются к WAN или LAN. Вам нужно выстроить соответствие между сетевыми интерфейсами устройства CPE и OpenFlow-портами виртуального коммутатора с помощью интерфейсов SD-WAN.

Вы можете посмотреть таблицу сетевых интерфейсов в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы сетевых интерфейсов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **Сеть**.
- Для просмотра таблицы сетевых интерфейсов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Сеть**.

Информация о сетевых интерфейсах отображается в следующих столбцах таблицы:

- **Переопределить**:
  - **Да** – параметры сетевого интерфейса уникальны и не наследуются из шаблона.
  - **Нет** – параметры сетевого интерфейса наследуются из шаблона.

  Этот столбец отображается только на устройстве CPE. Вы можете изменить значение этого столбца для каждого сетевого интерфейса непосредственно в таблице.
- **Включено**:
  - **Да** – сетевой интерфейс включен.
  - **Нет** – сетевой интерфейс выключен.

  Вы можете изменить значение этого столбца для каждого сетевого интерфейса непосредственно в таблице на устройстве CPE, предварительно установив для него значение **Да** в столбце **Переопределить**.
- **Унаследовано** – сетевой интерфейс унаследован из шаблона CPE:
  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.
- **Псевдоним** – псевдоним сетевого интерфейса для построения соответствия между сетевым интерфейсом и OpenFlow-портом. Вам нужно указать псевдоним сетевого интерфейса при создании интерфейса SD-WAN с типом WAN.
- **Описание** – описание сетевого интерфейса.
- **Зона** – зона межсетевого экрана.
- **NetFlow ifIndex** – постоянный числовой идентификатор интерфейса, используемый при отправке статистики по протоколу NetFlow.

  По умолчанию этот столбец скрыт.
- **Имя интерфейса** – имя физического порта или виртуального интерфейса операционной системы устройства CPE.

- **Протокол** – способ назначения сетевому интерфейсу IP-адреса:
  - **DHCP-клиент** – автоматически назначен IP-адрес по протоколу DHCP.
  - **Статический IPv4-адрес** – статически назначен IPv4-адрес.
  - **Статический IPv6-адрес** – статически назначен IPv6-адрес.
  - **QMI** – вручную указаны параметры подключения к LTE-сети.
  - **PPPoE** – вручную указаны параметры подключения к PPPoE-серверу.
  - **Отсутствует** – IP-адрес не назначен.
- **IP/маска** – IP-адрес, маска и шлюз по умолчанию сетевого интерфейса.
- **MTU** – значение MTU для сетевого интерфейса.
- **Включать автоматически** – сетевой интерфейс автоматически включается при включении устройства CPE:
  - **Да**.
  - **Нет**.

Действия, которые вы можете выполнить с таблицами, описаны в инструкции Работа с таблицами компонентов решения.

Создание сетевых интерфейсов

Вы можете создать сетевой интерфейс в шаблоне CPE или на устройстве CPE. Сетевой интерфейс, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Создание сетевого интерфейса с автоматическим назначением IP-адреса по протоколу DHCP

Чтобы создать сетевой интерфейс с автоматическим назначением IP-адреса по протоколу DHCP:

1. Перейдите к созданию сетевого интерфейса одним из следующих способов:
   - Если вы хотите создать сетевой интерфейс в шаблоне CPE, перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.
   - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Сеть**.

   Отобразится таблица сетевых интерфейсов.
2. Нажмите на кнопку **+ Сетевой интерфейс**.

3. В открывшемся окне в поле **Псевдоним** введите имя сетевого интерфейса для построения соответствия между сетевым интерфейсом OpenFlow-портом. Вам нужно указать имя сетевого интерфейса при создании интерфейса SD-WAN с типом WAN. Максимальная длина имени: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина имени: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких интерфейсов введите их имена через пробел.

   Если вы хотите назначить внешнюю метку VLAN сетевому интерфейсу, введите точку (.) после имени физического порта или виртуального интерфейса операционной системы, после чего введите внешнюю метку VLAN. Например, вы можете ввести `eth2.150`.

6. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.Если вы хотите создать мост из физических или виртуальных интерфейсов, имена которых указаны в поле **Имя интерфейса**, выполните следующие действия:

   a. Установите флажок **Мост**. Этот флажок снят по умолчанию.

   b. Если вы хотите использовать на мосту протокол STP для предотвращения петель маршрутизации, установите флажок **STP**. Этот флажок снят по умолчанию.

   c. В поле **Возраст (сек.)** введите время в секундах, в течение которого динамические записи хранятся в MAC-таблице моста. Если вы хотите использовать мост как хаб (англ. hub), введите `0` в этом поле. Диапазон значений: от 0 до 86 400.

7. Если вы хотите включить протокол NetFlow на сетевом интерфейсе, установите флажок **NetFlow**. Этот флажок снят по умолчанию.

8. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.

9. В раскрывающемся списке **Протокол** выберите **DHCP-клиент**.

10. Если вы не хотите, чтобы сетевой интерфейс автоматически включался одновременно с устройством CPE, снимите флажок **Включать автоматически**. Этот флажок установлен по умолчанию.

11. Если вы хотите, чтобы сетевому интерфейсу автоматически назначался IP-адрес, маршрут и шлюз по умолчанию, установите флажок **Назначать IP, маршрут и шлюз**. Этот флажок снят по умолчанию.

12. Если вы не хотите, чтобы на сетевом интерфейсе по умолчанию использовался маршрут, полученный по протоколу DHCP, снимите флажок **Использовать маршрут по умолчанию**. Этот флажок установлен по умолчанию.

13. При необходимости укажите DNS-сервер для сетевого интерфейса:

    a. В блоке **DNS-серверы** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите IP-адрес DNS-сервера.

    DNS-сервер будет указан и отобразится в блоке **DNS-серверы**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на значок удаления ✕.

14. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет фактический MAC-адрес сетевого интерфейса. Поле недоступно для изменения, если установлен флажок **Генерировать MAC автоматически**.

15. В поле **Переопределить MTU** введите значение MTU для сетевого интерфейса. Введенное значение заменяет MTU по умолчанию.

16. Если вы хотите, чтобы MAC-адрес сетевого интерфейса генерировался автоматически, установите флажок **Генерировать MAC автоматически** (снят по умолчанию).

17. В поле **Метрика маршрута** при необходимости введите метрику маршрута по умолчанию для сетевого интерфейса. Устройство CPE использует маршрут по умолчанию с наименьшей метрикой.

    Метрика маршрута для сетевых интерфейсов с псевдонимами **sdwan0** – **sdwan3** назначается автоматически при загрузке CPE: наибольший приоритет имеет интерфейс **sdwan0**, наименьший – **sdwan3.** В этом случае устройство CPE использует маршрут по умолчанию сетевого интерфейса **sdwan0**. Если сетевой интерфейс **sdwan0** выходит из строя, следующим используется маршрут по умолчанию сетевого интерфейса **sdwan1**, а после него – маршрут по умолчанию сетевого интерфейса **sdwan2**. При этом значение в поле **Метрика маршрута** заблокировано для изменения вручную у интерфейсов с псевдонимами **sdwan0** – **sdwan9**.

    Автоматический расчет метрики выполняется исходя из следующих признаков:

    - `1-4` при отсутствии ошибок и наличии доступа в интернет;
    - `11-14` при отсутствии ошибок и отсутствии доступа в интернет;
    - `21-24` при наличии ошибок и отсутствии доступа в интернет.

    Автоматическое назначение метрик интерфейсам выполняется в зависимости от цифры в конце псевдонима интерфейса по следующей схеме:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

18. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

19. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Создание сетевого интерфейса со статическим IPv4-адресом

Чтобы создать сетевой интерфейс со статическим IPv4-адресом:

1. Перейдите к созданию сетевого интерфейса одним из следующих способов:

   - Если вы хотите создать сетевой интерфейс в шаблоне CPE, перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.
   - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Сеть**.

   Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **+ Сетевой интерфейс**.
3. В открывшемся окне в поле **Псевдоним** введите имя сетевого интерфейса для построения соответствия между сетевым интерфейсом OpenFlow-портом. Вам нужно указать имя сетевого интерфейса при создании интерфейса SD-WAN с типом WAN. Максимальная длина имени: 15 символов.
4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите созданную зону межсетевого экрана.
5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина имени: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких интерфейсов введите их имена через пробел.

   Если вы хотите назначить внешнюю метку VLAN сетевому интерфейсу, введите точку (.) после имени физического порта или виртуального интерфейса операционной системы, после чего введите внешнюю метку VLAN. Например, вы можете ввести `eth2.150`.
6. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.Если вы хотите создать мост из физических или виртуальных интерфейсов, имена которых указаны в поле **Имя интерфейса**, выполните следующие действия:

   a. Установите флажок **Мост**. Этот флажок снят по умолчанию.

   b. Если вы хотите использовать на мосту протокол STP для предотвращения петель маршрутизации, установите флажок **STP**. Этот флажок снят по умолчанию.

   c. В поле **Возраст (сек.)** введите время в секундах, в течение которого динамические записи хранятся в MAC-таблице моста. Если вы хотите использовать мост как хаб (англ. hub), введите `0` в этом поле. Диапазон значений: от 0 до 86 400.
7. Если вы хотите включить протокол NetFlow на сетевом интерфейсе, установите флажок **NetFlow**. Этот флажок снят по умолчанию.
8. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.
9. В раскрывающемся списке **Протокол** выберите **Статический IPv4-адрес**.

10. Если вы не хотите, чтобы сетевой интерфейс автоматически включался одновременно с устройством CPE, снимите флажок **Включать автоматически**. Этот флажок установлен по умолчанию.

11. Если вы хотите, чтобы сетевому интерфейсу автоматически назначался IP-адрес, маршрут и шлюз по умолчанию, установите флажок **Назначать IP, маршрут и шлюз**. Этот флажок снят по умолчанию.

12. В раскрывающемся списке **Тип вводимого IPv4-адреса и маски подсети** выберите способ назначения IPv4-адреса сетевому интерфейсу:

    - **Вручную** – вручную назначить IPv4-адрес. При выборе этого значения выполните следующие действия:

      a. В поле **IPv4-адрес** введите IPv4-адрес сетевого интерфейса.

      b. В поле **IPv4-маска** введите маску подсети сетевого интерфейса.

      Это значение выбрано по умолчанию.

    - **Из пула IP-адресов** – назначить IPv4-адрес из указанного диапазона IP-адресов. При выборе этого значения в раскрывающемся списке **Диапазон IP** выберите созданный диапазон IP-адресов.

    - **Из пула подсетей** – назначить IPv4-адрес из указанного диапазона подсетей. При выборе этого значения в раскрывающемся списке **Диапазон подсетей** выберите созданный диапазон подсетей.

13. В поле **IPv4-шлюз** введите IPv4-адрес шлюза по умолчанию.

14. В поле **IPv4-трансляция** введите широковещательный адрес сетевого интерфейса. Если вы не указываете значение для этого параметра, оно генерируется автоматически.

15. При необходимости укажите DNS-сервер для сетевого интерфейса:

    a. В блоке **DNS-серверы** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите IP-адрес DNS-сервера.

    DNS-сервер будет указан и отобразится в блоке **DNS-серверы**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на значок удаления ✕.

16. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет фактический MAC-адрес сетевого интерфейса.

17. В поле **Переопределить MTU** введите значение MTU для сетевого интерфейса. Введенное значение заменяет MTU по умолчанию.

18. В поле **Метрика маршрута** при необходимости введите метрику маршрута по умолчанию для сетевого интерфейса. Устройство CPE использует маршрут по умолчанию с наименьшей метрикой.

    Метрика маршрута для сетевых интерфейсов с псевдонимами **sdwan0** – **sdwan3** назначается автоматически при загрузке CPE: наибольший приоритет имеет интерфейс **sdwan0**, наименьший – **sdwan3.** В этом случае устройство CPE использует маршрут по умолчанию сетевого интерфейса **sdwan0**. Если сетевой интерфейс **sdwan0** выходит из строя, следующим используется маршрут по умолчанию сетевого интерфейса **sdwan1**, а после него – маршрут по умолчанию сетевого интерфейса **sdwan2**. При этом значение в поле **Метрика маршрута** заблокировано для изменения вручную у интерфейсов с псевдонимами **sdwan0** – **sdwan9**.

    Автоматический расчет метрики выполняется исходя из следующих признаков:

    - `1-4` при отсутствии ошибок и наличии доступа в интернет;
    - `11-14` при отсутствии ошибок и отсутствии доступа в интернет;
    - `21-24` при наличии ошибок и отсутствии доступа в интернет.

    Автоматическое назначение метрик интерфейсам выполняется в зависимости от цифры в конце псевдонима интерфейса по следующей схеме:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

19. В блоке **DHCP-сервер** в раскрывающемся списке **Тип** выберите режим работы DHCP-сервера для сетевого интерфейса:

    - **Выключен**. Это значение выбрано по умолчанию.
    - **Ретранслятор**. При выборе этого значения в поле **IP DHCP-сервера** введите IP-адрес DHCP-сервера.
    - **Сервер**.

20. Если в раскрывающемся списке **Тип** вы выбрали **Сервер**, укажите параметры DHCP-сервера:

    a. В поле **Первый IP** введите, на сколько требуется сместиться от базового IP-адреса сетевого интерфейса для расчета минимального IP-адреса, который можно предоставить в аренду клиентам. Значение по умолчанию: `100`. Вы можете ввести значение больше 255 для больших подсетей.

    b. В поле **Лимит** введите максимальное количество IP-адресов, которое может быть выдано клиентам. Диапазон значений: от 1 до 250. Значение по умолчанию: `150`.

    c. В поле **Время аренды** введите максимальное время в часах, в течение которого отдельный IP-адрес может быть арендован клиентом. Диапазон значений: от 1 до 250. Значение указывается в формате `<количество часов>h`. Например, если вы хотите, чтобы максимальное время аренды составляло 5 часов, введите `5h`. Значение по умолчанию: `12h`.

    d. При необходимости укажите DHCP-опцию:

        1. В блоке **DHCP-опции** нажмите на кнопку **+ Добавить**.

        2. В отобразившемся поле введите номер DHCP-опции в соответствии со стандартом RFC 1533. Максимальная длина: 250 символов.

    DHCP-опция будет указана и отобразится в блоке **DHCP-опции**. Вы можете указать несколько DHCP-опций и удалить DHCP-опции. Для удаления DHCP-опции нажмите рядом с ней на значок удаления ✕.

21. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

22. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Создание сетевого интерфейса со статическим IPv6-адресом

Чтобы создать сетевой интерфейс со статическим IPv6-адресом:

1. Перейдите к созданию сетевого интерфейса одним из следующих способов:

    - Если вы хотите создать сетевой интерфейс в шаблоне CPE, перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.
    - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Сеть**.

    Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **+ Сетевой интерфейс**.

3. В открывшемся окне в поле **Псевдоним** введите имя сетевого интерфейса для построения соответствия между сетевым интерфейсом OpenFlow-портом. Вам нужно указать имя сетевого интерфейса при создании интерфейса SD-WAN с типом WAN. Максимальная длина имени: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина имени: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких интерфейсов введите их имена через пробел.

   Если вы хотите назначить внешнюю метку VLAN сетевому интерфейсу, введите точку (.) после имени физического порта или виртуального интерфейса операционной системы, после чего введите внешнюю метку VLAN. Например, вы можете ввести `eth2.150`.

6. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.Если вы хотите создать мост из физических или виртуальных интерфейсов, имена которых указаны в поле **Имя интерфейса**, выполните следующие действия:

   a. Установите флажок **Мост**. Этот флажок снят по умолчанию.

   b. Если вы хотите использовать на мосту протокол STP для предотвращения петель маршрутизации, установите флажок **STP**. Этот флажок снят по умолчанию.

   c. В поле **Возраст (сек.)** введите время в секундах, в течение которого динамические записи хранятся в MAC-таблице моста. Если вы хотите использовать мост как хаб (англ. hub), введите `0` в этом поле. Диапазон значений: от 0 до 86 400.

7. Если вы хотите включить протокол NetFlow на сетевом интерфейсе, установите флажок **NetFlow**. Этот флажок снят по умолчанию.

8. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.

9. В раскрывающемся списке **Протокол** выберите **Статический IPv6-адрес**.

10. Если вы не хотите, чтобы сетевой интерфейс автоматически включался одновременно с устройством CPE, снимите флажок **Включать автоматически**. Этот флажок установлен по умолчанию.

11. Если вы хотите, чтобы сетевому интерфейсу автоматически назначался IP-адрес, маршрут и шлюз по умолчанию, установите флажок **Назначать IP, маршрут и шлюз**. Этот флажок снят по умолчанию.

12. В поле **IPv6-адрес** введите IPv6-адрес сетевого интерфейса. Вы можете ввести несколько адресов через пробел.

13. В поле **IPv6-суффикс** введите IPv6-суффикс сетевого интерфейса. Максимальная длина: 30 символов.

14. В поле **IPv6-шлюз** введите IPv6-адрес шлюза по умолчанию.

15. В поле **Длина префикса** введите длину IPv6-префикса сетевого интерфейса. Диапазон значений: 12 до 127.

16. В поле **Суб-префикс DHCPv6** введите размер суб-префикса DHCPv6 сетевого интерфейса. Максимальная длина: 256 символов.

17. В поле **IPv6-префикс** введите IPv6-префикс сетевого интерфейса. Максимальная длина: 30 символов.

18. Если вы хотите, чтобы сетевой интерфейс принимал указанный класс IPv6-префиксов, выполните следующие действия:

    a. В блоке **Класс IPv6** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите имя класса IPv6-префиксов. Максимальная длина: 256 символов.

    Класс IPv6-префиксов будет указан и отобразится в блоке **Класс IPv6**. Вы можете указать несколько классов IPv6-префиксов и удалить классы IPv6-префиксов. Для удаления класса IPv6-префиксов нажмите рядом с ним на значок удаления ✕.

19. При необходимости укажите DNS-сервер для сетевого интерфейса:

    a. В блоке **DNS-серверы** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите IP-адрес DNS-сервера.

    DNS-сервер будет указан и отобразится в блоке **DNS-серверы**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на значок удаления ✕.

20. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет фактический MAC-адрес сетевого интерфейса.

21. В поле **Переопределить MTU** введите значение MTU для сетевого интерфейса. Введенное значение заменяет MTU по умолчанию.

22. В поле **Метрика маршрута** при необходимости введите метрику маршрута по умолчанию для сетевого интерфейса. Устройство CPE использует маршрут по умолчанию с наименьшей метрикой.

    Метрика маршрута для сетевых интерфейсов с псевдонимами **sdwan0** – **sdwan3** назначается автоматически при загрузке CPE: наибольший приоритет имеет интерфейс **sdwan0**, наименьший – **sdwan3.** В этом случае устройство CPE использует маршрут по умолчанию сетевого интерфейса **sdwan0**. Если сетевой интерфейс **sdwan0** выходит из строя, следующим используется маршрут по умолчанию сетевого интерфейса **sdwan1**, а после него – маршрут по умолчанию сетевого интерфейса **sdwan2**. При этом значение в поле **Метрика маршрута** заблокировано для изменения вручную у интерфейсов с псевдонимами **sdwan0** – **sdwan9**.

    Автоматический расчет метрики выполняется исходя из следующих признаков:

    - `1-4` при отсутствии ошибок и наличии доступа в интернет;
    - `11-14` при отсутствии ошибок и отсутствии доступа в интернет;
    - `21-24` при наличии ошибок и отсутствии доступа в интернет.

    Автоматическое назначение метрик интерфейсам выполняется в зависимости от цифры в конце псевдонима интерфейса по следующей схеме:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

23. В блоке **DHCP-сервер** в раскрывающемся списке **Тип** выберите режим работы DHCP-сервера для сетевого интерфейса:

    - **Выключен**. Это значение выбрано по умолчанию.
    - **Ретранслятор**. При выборе этого значения в поле **IP DHCP-сервера** введите IP-адрес DHCP-сервера.
    - **Сервер**.

24. Если в раскрывающемся списке **Тип** вы выбрали **Сервер**, укажите параметры DHCP-сервера:

    a. В поле **Первый IP** введите, на сколько требуется сместиться от базового IP-адреса сетевого интерфейса для расчета минимального IP-адреса, который можно предоставить в аренду клиентам. Значение по умолчанию: `100`. Вы можете ввести значение больше 255 для больших подсетей.

    b. В поле **Лимит** введите максимальное количество IP-адресов, которое может быть выдано клиентам. Диапазон значений: от 1 до 250. Значение по умолчанию: `150`.

    c. В поле **Время аренды** введите максимальное время в часах, в течение которого отдельный IP-адрес может быть арендован клиентом. Диапазон значений: от 1 до 250. Значение указывается в формате `<количество часов>h`. Например, если вы хотите, чтобы максимальное время аренды составляло 5 часов, введите `5h`. Значение по умолчанию: `12h`.

    d. При необходимости укажите DHCP-опцию:

        1. В блоке **DHCP-опции** нажмите на кнопку **+ Добавить**.
        2. В отобразившемся поле введите номер DHCP-опции в соответствии со стандартом RFC 1533. Максимальная длина: 250 символов.

    DHCP-опция будет указана и отобразится в блоке **DHCP-опции**. Вы можете указать несколько DHCP-опций и удалить DHCP-опции. Для удаления DHCP-опции нажмите рядом с ней на значок удаления ✕.

25. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

26. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Создание сетевого интерфейса для подключения к LTE-сети

Данный функционал поддерживается не всеми моделями. За консультацией рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

Чтобы создать сетевой интерфейс для подключения к LTE-сети:

1. Перейдите к созданию сетевого интерфейса одним из следующих способов:

   - Если вы хотите создать сетевой интерфейс в шаблоне CPE, перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.
   - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Сеть**.

   Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **+ Сетевой интерфейс**.
3. В открывшемся окне в поле **Псевдоним** введите псевдоним сетевого интерфейса для построения соответствия между сетевым интерфейсом и OpenFlow-портом. Вам нужно указать псевдоним сетевого интерфейса при создании интерфейса SD-WAN с типом WAN. Максимальная длина псевдонима – 15 символов.
4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите созданную зону межсетевого экрана.
5. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.
6. В раскрывающемся списке **Протокол** выберите **QMI**.
7. В поле **Имя QMI** введите путь к модему на устройстве CPE. Максимальная длина пути: 30 символов. Например, вы можете ввести `/dev/cdc-wdm0`.
8. В списке **Источник APN** выберите источник ввода идентификатора APN оператора связи, выпустившего SIM-карту, установленную в модеме:

   - если вы хотите, чтобы APN подставился автоматически из справочника APN, выберите **Из справочника**, затем выберите нужный справочник в появившемся списке **Справочник APN**;
   - если вы хотите указать строку APN вручную, выберите **Вручную**, затем введите строку APN в появившемся поле **Строка APN**. Максимальная длина идентификатора – 30 символов.

9. В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации на сетевом интерфейсе:

   - **PAP** (Password Authentication Protocol).
   - **CHAP** (Challenge-Handshake Authentication Protocol).
   - **PAP и CHAP** – на сетевом интерфейсе используются оба вида аутентификации.
   - **Отсутствует** – на сетевом интерфейсе не используется аутентификация.

10. В поле **Имя пользователя для аутентификации PAP/CHAP** введите имя пользователя для PAP/CHAP-аутентификации. Максимальная длина имени: 30 символов. Если вы не хотите использовать аутентификацию, не указывайте значение для этого параметра.

11. В поле **Пароль для аутентификации PAP/CHAP** введите пароль для PAP/CHAP-аутентификации. Максимальная длина пароля: 30 символов. Если вы не хотите использовать аутентификацию, не указывайте значение для этого параметра.

12. В поле **PIN-код** введите PIN-код SIM-карты, установленной в модеме. Максимальная длина PIN-кода: 4 цифры.

13. В поле **Задержка** введите время в секундах, по прошествии которого сетевой интерфейс начинает взаимодействовать с модемом. Максимальное значение: 30. Параметр используется, когда загрузка модема занимает слишком много времени.

14. При необходимости укажите режимы мобильной связи, в которых должен работать модем:

    a. В блоке **Режимы** нажмите на кнопку **+ Добавить**.

    b. В раскрывающемся списке выберите одно из следующих значений:

       - **All** – использовать все доступные режимы мобильной связи
       - **LTE**
       - **UMTS**
       - **GSM**
       - **CDMA**
       - **TD-SCDMA**

    Режимы мобильной связи будут заданы на модеме и отобразятся в блоке **Режимы**. Вы можете указать несколько режимов и удалить режимы. Для удаления режима нажмите рядом с ним на значок удаления ✕.

15. При необходимости укажите DNS-сервер для сетевого интерфейса:

    a. В блоке **DNS-серверы** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите IP-адрес DNS-сервера.

    DNS-сервер будет указан и отобразится в блоке **DNS-серверы**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на значок удаления ✕.

16. В поле **Профиль подключения** введите индекс профиля подключения, который сетевой интерфейс использует вместо идентификатора APN. Максимальная длина индекса: 30 символов.

17. В раскрывающемся списке **IP-стек** выберите IP-стек, который используется на сетевом интерфейсе:

    - **IPv4 –** использовать на сетевом интерфейсе стек протокола IPv4. Это значение выбрано по умолчанию.
    - **IPV6 –** использовать на сетевом интерфейсе стек протокола IPv6.
    - **Двойной стек (IPv4 и IPv6) –** использовать на сетевом интерфейсе двойной стек IPv4 и IPv6.

18. Снимите флажок **IPv4 через DHCP**, чтобы не назначать сетевому интерфейсу IPv4-адрес по протоколу DHCP. При необходимости установить флажок одновременно с флажком **IPv6 через DHCP** в раскрывающемся списке **IP-стек** выберите **Двойной стек (IPv4 и IPv6)**. Этот флажок установлен по умолчанию.

19. Установите флажок **IPv6 через DHCP**, чтобы назначить сетевому интерфейсу IPv6-адрес по протоколу DHCP. При необходимости установить флажок одновременно с флажком **IPv4 через DHCP** в раскрывающемся списке **IP-стек** выберите **Двойной стек (IPv4 и IPv6)**. Этот флажок снят по умолчанию.

20. Снимите флажок **Автоподключение**, чтобы не подключать автоматически модем к сети. Этот флажок установлен по умолчанию.

21. В поле **PLMN** введите идентификатор PLMN оператора связи. Первые три цифры идентификатора PLMN являются кодом страны (MCC, англ. Moblie Country Code), следующие две или три цифры – кодом мобильной сети (MNC, англ. Mobile Network Code). Например, для сети "Вымпелком" на территории Российской Федерации PLMN=25099: MCC = 250 (РФ), MNC = 99 (Вымпелком).

22. В поле **Время** введите время в секундах для ожидания сетевым интерфейсом выполнения операций на SIM-карте, установленной в модеме. Максимальное значение: 20. Значение по умолчанию: `10`.

23. В поле **Последовательный порт** введите имя последовательного порта (англ. serial port) модема. Максимальная длина имени: 50 символов.

24. В поле **Метрика маршрута** при необходимости введите метрику маршрута по умолчанию для сетевого интерфейса. Устройство CPE использует маршрут по умолчанию с наименьшей метрикой.

    Метрика маршрута для сетевых интерфейсов с псевдонимами **sdwan0** – **sdwan3** назначается автоматически при загрузке CPE: наибольший приоритет имеет интерфейс **sdwan0**, наименьший – **sdwan3.** В этом случае устройство CPE использует маршрут по умолчанию сетевого интерфейса **sdwan0**. Если сетевой интерфейс **sdwan0** выходит из строя, следующим используется маршрут по умолчанию сетевого интерфейса **sdwan1**, а после него – маршрут по умолчанию сетевого интерфейса **sdwan2**. При этом значение в поле **Метрика маршрута** заблокировано для изменения вручную у интерфейсов с псевдонимами **sdwan0** – **sdwan9**.

    Автоматический расчет метрики выполняется исходя из следующих признаков:

    - `1-4` при отсутствии ошибок и наличии доступа в интернет;
    - `11-14` при отсутствии ошибок и отсутствии доступа в интернет;
    - `21-24` при наличии ошибок и отсутствии доступа в интернет.

    Автоматическое назначение метрик интерфейсам выполняется в зависимости от цифры в конце псевдонима интерфейса по следующей схеме:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

25. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

26. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Создание сетевого интерфейса для подключения к PPPoE-серверу

Чтобы создать сетевой интерфейс для подключения к PPPoE-серверу:

1. Перейдите к созданию сетевого интерфейса одним из следующих способов:

    - Если вы хотите создать сетевой интерфейс в шаблоне CPE, перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.
    - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Сеть**.

    Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **+ Сетевой интерфейс**.

3. В открывшемся окне в поле **Псевдоним** введите имя сетевого интерфейса для построения соответствия между сетевым интерфейсом OpenFlow-портом. Вам нужно указать имя сетевого интерфейса при создании интерфейса SD-WAN с типом WAN. Максимальная длина имени: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина имени: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких интерфейсов введите их имена через пробел.

   Если вы хотите назначить внешнюю метку VLAN сетевому интерфейсу, введите точку (.) после имени физического порта или виртуального интерфейса операционной системы, после чего введите внешнюю метку VLAN. Например, вы можете ввести `eth2.150`.

6. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.В раскрывающемся списке **Протокол** выберите **PPPoE**.

7. В поле **Концентратор доступа** введите IP-адрес или имя хоста концентратора доступа, к которому подключается сетевой интерфейс. Максимальная длина имени хоста: 30 символов. Если вы не вводите значение в этом поле, Point-to-Point Protocol Daemon (далее PPPD) использует первый обнаруженный концентратор доступа.

8. В поле **Сервис** введите имя PPPoE-сервиса, к которому подключается сетевой интерфейс. Максимальная длина имени: 30 символов. Если вы не вводите значение в этом поле, PPPD использует первый обнаруженный PPPoE-сервис.

9. В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации на сетевом интерфейсе:

   - **PAP и CHAP** – на сетевом интерфейсе используется аутентификация PAP и CHAP. При выборе этого значения выполните следующие действия:

     a. В поле **Имя пользователя для аутентификации PAP/CHAP** введите имя пользователя для PAP/CHAP-аутентификации. Максимальная длина имени: 30 символов.

     b. В поле **Пароль для аутентификации PAP/CHAP** введите пароль для PAP/CHAP-аутентификации. Максимальная длина пароля: 30 символов.

   - **Отсутствует** – на сетевом интерфейсе не используется аутентификация.

10. В поле **Максимум неудачных пингов** введите количество безуспешных ICMP-запросов, при котором сетевой интерфейс считает PPPoE-сервер недоступным. Диапазон значений: от 1 до 3600. Значение по умолчанию: `5`.

11. В поле **Интервал пингов (сек.)** введите интервал времени в секундах для отправки сетевым интерфейсом ICMP-запросов PPPoE-серверу. Диапазон значений: от 1 до 3600. Значение по умолчанию: `1`.

12. Если вы хотите, чтобы сетевой интерфейс разрывал неактивное PPPoE-подключение по прошествии указанного времени, в поле **Время (сек.)** введите время в секундах. Диапазон значений: от 1 до 3600.

13. При необходимости в поле **Host-Uniq** введите тег Host-Uniq для PPPoE-подключения. Максимальная длина тега: 30 символов. Если не вводите значение в этом поле, в качестве тега Host-Uniq используется идентификатор PPPD-процесса (англ. PPPD process identifier).

14. В поле **Переопределить MTU** введите значение MTU для сетевого интерфейса. Введенное значение заменяет MTU по умолчанию.

15. В поле **Метрика маршрута** при необходимости введите метрику маршрута по умолчанию для сетевого интерфейса. Устройство CPE использует маршрут по умолчанию с наименьшей метрикой.

    Метрика маршрута для сетевых интерфейсов с псевдонимами **sdwan0** – **sdwan3** назначается автоматически при загрузке CPE: наибольший приоритет имеет интерфейс **sdwan0**, наименьший – **sdwan3.** В этом случае устройство CPE использует маршрут по умолчанию сетевого интерфейса **sdwan0**. Если сетевой интерфейс **sdwan0** выходит из строя, следующим используется маршрут по умолчанию сетевого интерфейса **sdwan1**, а после него – маршрут по умолчанию сетевого интерфейса **sdwan2**. При этом значение в поле **Метрика маршрута** заблокировано для изменения вручную у интерфейсов с псевдонимами **sdwan0** – **sdwan9**.

    Автоматический расчет метрики выполняется исходя из следующих признаков:

    - `1-4` при отсутствии ошибок и наличии доступа в интернет;
    - `11-14` при отсутствии ошибок и отсутствии доступа в интернет;
    - `21-24` при наличии ошибок и отсутствии доступа в интернет.

    Автоматическое назначение метрик интерфейсам выполняется в зависимости от цифры в конце псевдонима интерфейса по следующей схеме:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

16. При необходимости снимите следующие флажки:

    - Снимите флажок **Keepalive adaptive**, чтобы сетевой интерфейс, не получивший от PPPoE-сервера контрольные пакеты LCP (Link Control Protocol), разрывал PPPoE-подключение, даже если от PPPoE-сервера пришел трафик.
    - Снимите флажок **Использовать маршрут по умолчанию**, чтобы не использовать по умолчанию на сетевом интерфейсе маршрут, полученный от PPPoE-сервера.
    - Снимите флажок **Назначенный пиром DNS-сервер**, чтобы сетевой интерфейс не использовал DNS-серверы, назначенные его соседям.

    По умолчанию флажки установлены.

17. Если вы хотите передать дополнительные аргументы командной строки при запуске PPPD (Point-to-Point Protocol Daemon), в поле **PPPD** введите аргументы командной строки. Например, вы можете передать PPPD параметры аутентификации, IP-адреса и скрипты.

18. При необходимости укажите DNS-сервер для сетевого интерфейса:

    a. В блоке **DNS-серверы** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите IP-адрес DNS-сервера.

    DNS-сервер будет указан и отобразится в блоке **DNS-серверы**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на значок удаления ✕.

19. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

20. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Создание сетевого интерфейса без IP-адреса

Чтобы создать сетевой интерфейс без IP-адреса:

1. Перейдите к созданию сетевого интерфейса одним из следующих способов:

   - Если вы хотите создать сетевой интерфейс в шаблоне CPE, перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.
   - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Сеть**.

   Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **+ Сетевой интерфейс**.

3. В открывшемся окне в поле **Псевдоним** введите имя сетевого интерфейса для построения соответствия между сетевым интерфейсом OpenFlow-портом. Вам нужно указать имя сетевого интерфейса при создании интерфейса SD-WAN с типом WAN. Максимальная длина имени: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина имени: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких интерфейсов введите их имена через пробел.

   Если вы хотите назначить внешнюю метку VLAN сетевому интерфейсу, введите точку (.) после имени физического порта или виртуального интерфейса операционной системы, после чего введите внешнюю метку VLAN. Например, вы можете ввести `eth2.150`.

6. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.Если вы хотите создать мост из физических или виртуальных интерфейсов, имена которых указаны в поле **Имя интерфейса**, выполните следующие действия:

   a. Установите флажок **Мост**. Этот флажок снят по умолчанию.

   b. Если вы хотите использовать на мосту протокол STP для предотвращения петель маршрутизации, установите флажок **STP**. Этот флажок снят по умолчанию.

   c. В поле **Возраст (сек.)** введите время в секундах, в течение которого динамические записи хранятся в MAC-таблице моста. Если вы хотите использовать мост как хаб (англ. hub), введите `0` в этом поле. Диапазон значений: от 0 до 86 400.

7. Если вы хотите включить протокол NetFlow на сетевом интерфейсе, установите флажок **NetFlow**. Этот флажок снят по умолчанию.

8. В поле **NetFlow ifIndex** при необходимости укажите постоянный числовой идентификатор интерфейса, который будет использоваться при отправке статистики по протоколу NetFlow. Диапазон значений: от 1 до 65535.

9. В раскрывающемся списке **Протокол** выберите **Отсутствует**.

10. Если вы хотите обеспечить L2-связность между устройствами CPE, установите флажок **L2-режим**. Когда флажок установлен, на виртуальном коммутаторе устройства CPE автоматически создается OpenFlow-порт, ссылающийся на сетевой интерфейс. Этот флажок снят по умолчанию. Вы не можете установить флажок в следующих случаях:

    - При создании сетевого интерфейса вы установили один из следующих флажков:
        - **Мост**.
        - **NetFlow**.
        - **Назначать IP, маршрут и шлюз**.
    - Сетевой интерфейс используется в статическом маршруте.
    - Сетевой интерфейс используется протоколом BGP.
    - Сетевой интерфейс используется протоколом OSPF.
    - Сетевой интерфейс используется протоколом VRRP.
    - Сетевой интерфейс используется для передачи multicast-трафика.
    - Сетевой интерфейс используется виртуальной таблицей маршрутизации (VRF).
    - Сетевой интерфейс используется для диагностики устройства CPE с помощью утилиты ping, traceroute, tcpdump или sweep.

    Если вы установили флажок, номер OpenFlow-порта, который автоматически создается на виртуальном коммутаторе устройства CPE, отобразится в поле **OpenFlow-порт**. Вы можете изменить номер OpenFlow-порта. Диапазон значений: от 11 до 20.

11. Если вы хотите, чтобы сетевой интерфейс автоматически включался одновременно с устройством CPE, установите флажок **Включать автоматически**. Этот флажок снят по умолчанию.

12. Если вы хотите, чтобы сетевому интерфейсу автоматически назначался IP-адрес, маршрут и шлюз по умолчанию, установите флажок **Назначать IP, маршрут и шлюз**. Этот флажок снят по умолчанию.

13. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет фактический MAC-адрес сетевого интерфейса.

14. В поле **Переопределить MTU** введите значение MTU для сетевого интерфейса. Введенное значение заменяет MTU по умолчанию.

15. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

16. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение сетевого интерфейса

Вы можете изменить сетевой интерфейс в шаблоне CPE или на устройстве CPE. Сетевой интерфейс, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить сетевой интерфейс:

1. Перейдите к изменению сетевого интерфейса одним из следующих способов:

    - Если вы хотите изменить сетевой интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.
    - Если вы хотите изменить сетевой интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Сеть**. Если вы хотите изменить сетевой интерфейс, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с сетевым интерфейсом.

    Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **Изменить** рядом с сетевым интерфейсом, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры сетевого интерфейса. Описание параметров см. в инструкциях по созданию сетевого интерфейса.

4. Нажмите на кнопку **Сохранить**.

    Сетевой интерфейс будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Выключение и включение сетевого интерфейса

Вы можете выключить или включить сетевой интерфейс в шаблоне CPE или на устройстве CPE. Сетевой интерфейс, выключенный или включенный в шаблоне CPE, автоматически выключается или включается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы выключить или включить сетевой интерфейс:

1. Перейдите к выключению или включению сетевого интерфейса одним из следующих способов:

   - Если вы хотите выключить или включить сетевой интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.

   - Если вы хотите выключить или включить сетевой интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN**, нажмите на устройство CPE и выберите вкладку **Сеть**. Если вы хотите выключить или включить сетевой интерфейс, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с сетевым интерфейсом.

   Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **Выключить** или **Включить** рядом с сетевым интерфейсом, который вы хотите выключить или включить.

   Сетевой интерфейс будет выключен или включен.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Отмена применения параметров сетевых интерфейсов к устройству CPE

Чтобы не применять к устройству CPE параметры сетевых интерфейсов:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, к которому вы хотите не применять параметры сетевых интерфейсов.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Сеть**.

   Отобразится таблица сетевых интерфейсов.

4. Установите флажок **Игнорировать параметры сети**. Этот флажок снят по умолчанию.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

   К устройству CPE не будут применяться параметры сетевых интерфейсов.

Для применения к устройству CPE параметров сетевых интерфейсов вам нужно снять флажок **Игнорировать параметры сети**.

Удаление сетевого интерфейса

Вы можете удалить сетевой интерфейс в шаблоне CPE или на устройстве CPE. Сетевой интерфейс, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете удалить на устройстве CPE сетевой интерфейс, унаследованный из шаблона CPE.

Удаленные сетевые интерфейсы невозможно восстановить.

Чтобы удалить сетевой интерфейс:

1. Перейдите к удалению сетевого интерфейса одним из следующих способов:

   - Если вы хотите удалить сетевой интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Сеть**.
   - Если вы хотите удалить сетевой интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Сеть**.

   Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **Удалить** рядом с сетевым интерфейсом, который вы хотите удалить.
3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Сетевой интерфейс будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Защита от IP-спуфинга с помощью uRPF

Эта функция позволяет снизить воздействие атак, связанных с подменой IP-адресов источника (IP-спуфинга) с помощью алгоритма Unicast Reverse Path Forwarding (uRPF) на интерфейсах CPE.

Принцип работы uRPF

Алгоритм использует таблицу маршрутизации (FIB - Forwarding Information Base) для проверки пакетов следующим образом:

1. Прием пакета.

   Маршрутизатор получает пакет на интерфейсе.

2. Проверка источника.

   uRPF проверяет исходный IP-адрес пакета.

3. Обратный поиск.

   Маршрутизатор ищет в таблице FIB, через какой интерфейс он отправил бы ответный пакет этому источнику (обратный путь).

4. Обработка пакета. Дальнейшие действия зависят от выбранного режима работы uRPF:

   - Строгий режим (Strict Mode)

     Пакет должен прийти именно через тот интерфейс, который является лучшим маршрутом обратно к источнику. Если путь не совпадает, пакет отбрасывается.

     Строгий режим используется для защиты от IP-спуфинга на периметре в сетях с симметричной маршрутизацией.

   - Облегченный режим (Loose Mode)

     Пакет принимается, если в таблице маршрутизации есть хоть какой-то маршрут к источнику, независимо от интерфейса.

     Облегченный режим может использоваться в сетях с асимметричной маршрутизацией (когда путь "туда" отличается от пути "обратно").

Вы можете настроить механизм uRPF отдельно для каждого сетевого интерфейса устройства CPE. Можно использовать механизм как на обычных интерфейсах, так и на интерфейсах типа bridge.

> Механизм uRPF доступен для интерфейсов с протоколами "DHCP-клиент" / "Статический IPv4-адрес" / "QMI" / "PPPoE" и недоступен для интерфейсов с протоколами "Статический IPv6-адрес" / "Отсутствует".

Вы можете настроить механизм uFPF как на самих устройствах CPE, так и в шаблонах CPE.

Чтобы настроить механизм uRPF:

1. Перейдите к настройке механизма uRPF одним из следующих способов:

   - Чтобы настроить механизм uRPF на устройстве CPE, в меню оркестратора перейдите в раздел **SD-WAN**, выберите устройство CPE и перейдите в раздел параметров **Сеть**.

   - Чтобы настроить механизм uRPF в шаблоне CPE, перейдите в меню оркестратора перейдите в раздел `Шаблоны CPE`, выберите шаблон CPE и перейдите в раздел параметров **Сеть**.

2. Создайте новый сетевой интерфейс или отредактируйте существующий.

   Если интерфейс используется в шаблоне CPE, включите для него переключатель **Переопределить**.

3. Если вы создаете новый сетевой интерфейс, выберите в выпадающем списке **Протокол** один из поддерживаемых протоколов:

   - **DHCP-клиент**
   - **Статический IPv4-адрес**
   - **QMI**
   - **PPPoE**

4. В выпадающем списке **Режим uRPF** выберите режим работы uRPF:

   - **Строгий**
   - **Облегченный**

5. Сохраните параметры сетевого интерфейса.

6. Примените изменения на устройстве или шаблоне CPE

Работа с интерфейсами SD-WAN

Интерфейсы SD-WAN – это логические интерфейсы над сетевыми интерфейсами устройства CPE и OpenFlow-портами виртуального коммутатора, образующие дополнительный уровень абстракции. Каждый интерфейс SD-WAN ссылается на сетевой интерфейс по имени сетевого интерфейса и на OpenFlow-порт по номеру OpenFlow-порта. Существуют следующие типы интерфейсов SD-WAN:

- Интерфейсы SD-WAN с типом LAN – созданные по умолчанию интерфейсы SD-WAN, ссылающиеся на сетевые интерфейсы, которые подключены к LAN. Вы не можете удалить и создать интерфейс SD-WAN с типом LAN, но можете изменить его, чтобы указать максимальную скорость и настроить очереди трафика.

- Интерфейсы SD-WAN с типом WAN – интерфейсы SD-WAN, ссылающиеся на сетевые интерфейсы, которые подключены к WAN.

- Интерфейс SD-WAN с типом management – созданный по умолчанию интерфейс SD-WAN, ссылающийся на сетевой интерфейс, который используется для пассивного мониторинга устройства CPE системой мониторинга Zabbix, а также для подключения оркестратора к устройству CPE по протоколу SSH. Вы не можете удалить и создать интерфейс SD-WAN с типом management.

Вы можете посмотреть таблицу интерфейсов SD-WAN в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы интерфейсов SD-WAN в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **SD-WAN → Интерфейсы**.

- Для просмотра таблицы интерфейсов SD-WAN на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **SD-WAN → Интерфейсы**.

Информация об интерфейсах SD-WAN отображается в следующих столбцах таблицы:

- **Тип** – тип интерфейса SD-WAN:
  - **WAN**.
  - **LAN**.
  - **Management**.
- **Унаследовано** – интерфейс SD-WAN унаследован из шаблона CPE:
  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.
- **Порт** – номер OpenFlow-порта.
- **Псевдоним** – имя сетевого интерфейса.
- **Максимальная скорость** – максимальная скорость интерфейса SD-WAN в мегабитах в секунду.

Дополнительная информация о проверках WAN, к которым подключены интерфейсы SD-WAN с типом WAN отображается в следующих столбцах таблицы:

- **IP для отслеживания** – IP-адреса хостов для проверки доступности WAN.
- **Надежность** – минимальное количество успешных проверок для признания WAN доступной.
- **Количество** – количество запросов хостам в рамках одной проверки WAN.
- **Время** – время ожидания ответа от хостов в миллисекундах.
- **Интервал (сек.)** – интервал времени для проверки WAN в секундах.
- **Не работает** – количество безуспешных проверок для признания WAN недоступной.
- **Работает** – количество успешных проверок для признания WAN доступной.
- **Мониторинг скорости** – скорость интерфейса SD-WAN с типом WAN измеряется:
  - **Да**.
  - **Нет**.

О передаче контроллеру информации об интерфейсах SD-WAN с типом WAN

При создании создании или изменении интерфейсов SD-WAN с типом WAN вы можете указать, какую информацию требуется передать контроллеру.

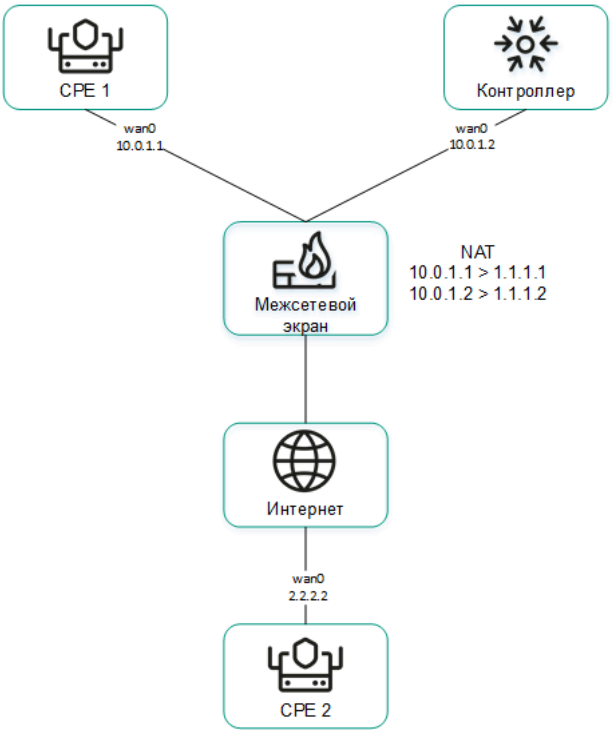
Передача контроллеру публичных IP-адресов и UDP-портов интерфейсов SD-WAN с типом WAN

Для построения соединений между устройствами CPE контроллеру необходимо получить информацию о публичных IP-адресах интерфейсов SD-WAN с типом WAN. По умолчанию контроллер получает эту информацию с помощью управляющей сессии. В этом случае в качестве публичного IP-адреса используется IP-адрес источника.

Вы можете указать IP-адреса и UDP-порты интерфейсов SD-WAN с типом WAN вручную. На рисунке ниже устройство CPE 1 и контроллер находятся в одной локальной сети и выходят в интернет, используя один межсетевой экран, который транслирует IP-адреса.

Если при установке сессии между интерфейсом SD-WAN с типом WAN устройства CPE 1 и публичным IP-адресом контроллера (1.1.1.2) межсетевой экран невозможно настроить таким образом, чтобы контроллер транслировал частный IP-адрес в публичный (10.0.1.1 > 1.1.1.1), контроллер не в состоянии получить информацию о публичном IP-адресе интерфейса SD-WAN с типом WAN и передать его другим устройствам CPE в топологии (устройство CPE 2).

В результате между устройствами CPE 1 и 2 невозможно построить соединение, устройство CPE 1 становится изолированным и не может быть добавлено в общую плоскость управления сетью.



Устройство CPE 1 и контроллер находятся за NAT и связаны с устройством CPE 2

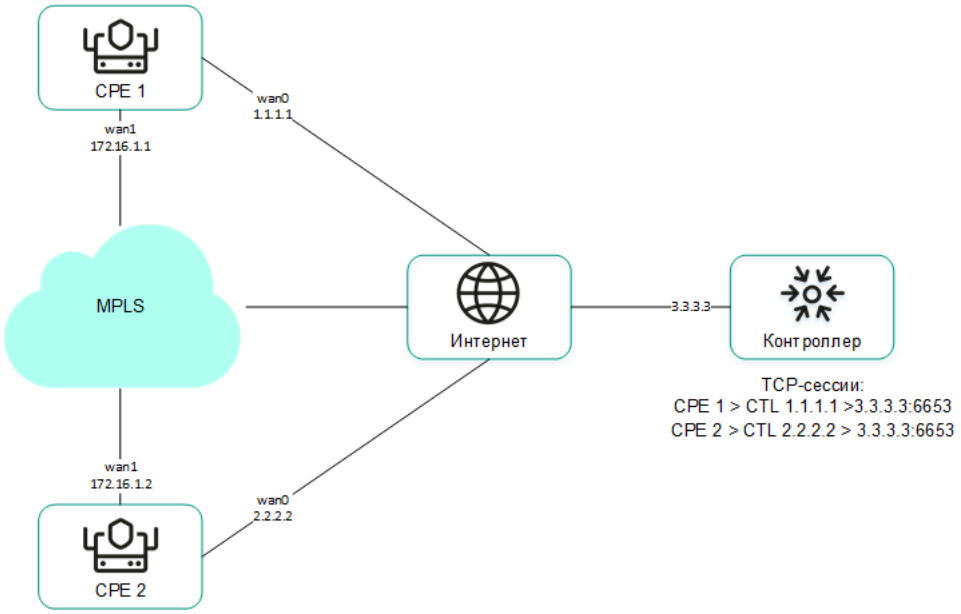
Передача контроллеру IP-адресов интерфейсов SD-WAN с типом WAN, находящихся в изолированной сети

Интерфейсы SD-WAN с типом WAN могут находиться в изолированной сети без возможности установить управляющую сессию с контроллером, но при этом они могут быть использованы для построения соединений. В этом случае контроллер не может получить информацию об IP-адресах изолированных интерфейсов SD-WAN с типом WAN и использовать ее для построения соединений между устройствами CPE.

На рисунке ниже устройства CPE 1 и 2 имеют по два интерфейса SD-WAN с типом WAN, но могут установить управляющую сессию с контроллером только через wan0, так как wan1 находятся в изолированной сети (MPLS), которая не имеет доступа к контроллеру. При этом оба wan1 могут быть использованы, чтобы построить соединение.

Если у одного из устройств CPE выходит из строя соединение для взаимодействия с контроллером, все остальные соединения также не могут быть использованы, даже если они сохраняют работоспособность, так как контроллер исключает устройство из топологии.

IP-адреса изолированных интерфейсов SD-WAN с типом WAN передаются контроллеру через оркестратор.



Устройства CPE 1`и 2 связаны друг с другом через MPLS, а также с контроллером через интернет

Фрагментация пакетов

Kaspersky SD-WAN проверяет, поддерживается ли фрагментация пакетов трафика на устройствах CPE. Проверка фрагментации пакетов запускается автоматически. При включении каждое устройство CPE отправляет два ICMP-запроса на IP-адреса, которые вы указали при создании или изменении интерфейсов SD-WAN с типом WAN.

Отправленные ICMP-запросы имеют размер пакета 1600 байт. Если хотя бы один из ICMP-запросов получает ответ, проверка фрагментации пакетов на устройстве CPE считается успешной. Вы можете посмотреть результат проверки фрагментации в столбце **Фрагментация** таблицы устройств CPE или таблицы соединений.

Очереди трафика на интерфейсах SD-WAN

На интерфейсах SD-WAN может использоваться не более 8 очередей трафика. Для каждой очереди трафика вам нужно указать минимальную и максимальную скорость в процентах от общей скорости, указанной для интерфейса SD-WAN. Сумма всех указанных для очередей трафика значений минимальной скорости передачи не должна превышать 100%.

Очереди трафика имеют строгий приоритет, и не зарезервированная полоса пропускания сначала предлагается трафику из очереди с более высоким приоритетом. Каждой очереди трафика гарантируется минимальная полоса пропускания в соответствии с указанной для нее минимальной скоростью. Верхнее ограничение максимальной скорости для более приоритетных очередей трафика необходимо, чтобы предоставить доступ к полосе пропускания трафику из менее приоритетных очередей.

Вы можете настроить очереди трафика при создании интерфейса SD-WAN с типом WAN или изменении интерфейса SD-WAN.

Операторы связи (англ. service providers) могут использовать разные политики качества обслуживания для маркировки очередей трафика в своих сетях и выполнения требований SLA для пропуска клиентского трафика. Поэтому при одновременном подключении к сетям разных операторов связи устройства CPE могут перемаркировывать трафик из разных очередей для каждого интерфейса SD-WAN с типом WAN. Для настройки перемаркировки трафика вам нужно изменить значение типа обслуживания (англ. Type of Service, далее также ToS) при настройке очередей трафика на интерфейсе SD-WAN.

Вы можете изменить только значения ToS внешних заголовков пакетов трафика, исходящих из интерфейсов SD-WAN с типом WAN. Изменение недоступно для значений ToS внутренних заголовков пакетов трафика.

Создание интерфейса SD-WAN с типом WAN

Вы можете создать интерфейс SD-WAN с типом WAN в шаблоне CPE или на устройстве CPE. Интерфейс SD-WAN с типом WAN, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать интерфейс SD-WAN с типом WAN:

1. Перейдите к созданию интерфейса SD-WAN с типом WAN одним из следующих способов:

   - Если вы хотите создать интерфейс SD-WAN с типом WAN в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **SD-WAN → Интерфейсы**.

   - Если вы хотите создать интерфейс SD-WAN с типом WAN на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

2. Нажмите на кнопку **+ Добавить**.

3. В открывшемся окне в поле **OpenFlow-порт** введите номер OpenFlow-порта, который создается на виртуальном коммутаторе.

4. В поле **Интерфейс (псевдоним)** введите псевдоним созданного сетевого интерфейса, на который ссылается интерфейс SD-WAN с типом WAN.

5. В поле **Максимальная скорость** введите максимальную скорость интерфейса SD-WAN с типом WAN в мегабитах в секунду. Диапазон значений: от 1 до 100 000. Значение по умолчанию: `1000`.

6. Настройте проверку доступности WAN, к которой подключен интерфейс SD-WAN с типом WAN:

   a. Укажите хост для проверки доступности WAN. Для этого в блоке **IP для отслеживания** введите IP-адрес хоста и нажмите на кнопку **+ Добавить**.

      Хост будет указан и отобразится в блоке **IP для отслеживания**. Вы можете указать несколько хостов и удалить хосты. Для удаления хоста нажмите рядом с ним на значок удаления ✕.

   b. В поле **IP для проверки фрагментации** введите IPv4-адрес хоста, до которого проверяется поддержка фрагментации. Значение по умолчанию: `1.1.1.1`.

   c. В поле **Надежность** введите минимальное количество успешных проверок для признания WAN доступной. Значение по умолчанию: `1`.

      Вам нужно убедиться, что количество хостов не превышает количество IP-адресов, указанных в блоке **IP для отслеживания**. В противном случае WAN всегда будет считаться недоступной.

   d. В поле **Интервал (сек.)** введите интервал времени в секундах для проверки WAN. Диапазон значений: от 1 до 600. Значение по умолчанию: `2`.

   e. В поле **Количество** введите количество запросов хостам в рамках одной проверки WAN. Диапазон значений: от 1 до 600. Значение по умолчанию: `2`.

   f. В поле **Время** введите время ожидания ответа от хостов в миллисекундах. Диапазон значений: от 1 до 100 000. Значение по умолчанию: `2000`.

   g. В поле **Не работает** введите количество безуспешных проверок для признания WAN недоступной. Диапазон значений: от 1 до 600. Значение по умолчанию: `3`.

   h. В поле **Работает** введите количество успешных проверок для признания WAN доступной. Диапазон значений: от 1 до 600. Значение по умолчанию: `2`.

   i. В раскрывающемся списке **Мониторинг скорости** выберите, измеряется ли скорость интерфейса SD-WAN с типом WAN:

      - **Да**.
      - **Нет**. Это значение выбрано по умолчанию.

7. Если вы хотите настроить очереди трафика на интерфейсе SD-WAN с типом WAN, выполните следующие действия:

   a. Выберите вкладку **QoS**.

      Отобразится таблица очередей трафика.

   b. В столбце **Изменить ToS** выберите значение Type of Service внешних заголовков пакетов трафика каждой очереди.

   c. В столбце **Минимальная скорость (%)** укажите минимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN с типом WAN. Сумма значений в столбце не должна превышать 100.

   d. В столбце **Максимальная скорость (%)** укажите максимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN с типом WAN. Параметр используется для того, чтобы трафик очередей с высоким приоритетом постоянно не вытеснял трафик очередей с низким приоритетом.

   Максимальная скорость интерфейса SD-WAN с типом WAN указывается на шаге 5 этой инструкции.

8. Если вы хотите настроить передачу контроллеру информации об интерфейсе SD-WAN с типом WAN, выполните следующие действия:

   a. Выберите вкладку **NAT и изолированные подлежащие WAN**.

   b. В раскрывающемся списке **Состояние** выберите одно из следующих значений:

      - **Выключено** – контроллеру не требуется передавать информацию об интерфейсе SD-WAN с типом WAN. Это значение выбрано по умолчанию.
      - **NAT/PAT** – интерфейс SD-WAN с типом WAN находится за NAT или PAT, и интерфейсу SD-WAN с типом WAN требуется назначить публичный IP-адрес и номер UDP-порта, после чего передать их контроллеру.
      - **Изолированная подлежащая WAN** – интерфейс SD-WAN с типом WAN подключен к изолированной сети, и IP-адрес интерфейса SD-WAN с типом WAN требуется передать контроллеру.

   c. Если в раскрывающемся списке **Состояние** вы выбрали **NAT/PAT**, выполните следующие действия:

      1. В поле **Реальный IP-адрес** введите публичный IPv4-адрес интерфейса SD-WAN с типом WAN.
      2. В поле **Реальный UDP GENEVE-порт** введите номер UDP-порта интерфейса SD-WAN с типом WAN. Диапазон значений: от 1 до 65 535.

   d. Если в раскрывающемся списке **Состояние** вы выбрали **Изолированная подлежащая WAN**, в поле **IP-адрес** введите IPv4-адрес интерфейса SD-WAN с типом WAN.

   e. Если необходимо, переопределите виртуальную таблицу маршрутизации для интерфейса SD-WAN с типом WAN. Для этого включите переключатель **Назначить VRF**, затем в выпадающем списке **VRF** выберите нужную виртуальную таблицу маршрутизации.

      Переопределение VRF позволяет задать альтернативный маршрут для связи с контроллером, например, использовать интерфейс с типом LAN вместо стандартного WAN. Значение, которое вы указали в списке **VRF**, вступит в силу только после перезагрузки CPE или включения/выключения соответствующего сетевого интерфейса.

9. Если интерфейсы SD-WAN с типом WAN устройства CPE подключены к разным сетям, например к интернету и частной MPLS-сети, вы можете изменить IP-адреса и номера TCP-портов узлов контроллера на отдельном интерфейсе SD-WAN с типом WAN. Для этого выполните следующие действия:

   a. Выберите вкладку **Контроллеры**.

   b. Установите флажок **Переписать IP/порт контроллеров**. Этот флажок снят по умолчанию.

   c. В раскрывающемся списке **Количество контроллеров** выберите количество узлов контроллера.

   > Вам нужно указать количество узлов контроллера, которые вы развернули при развертывании экземпляра SD-WAN. В противном случае происходит ошибка и данные остаются прежними.

   d. В поле **IP-адрес** введите IPv4-адрес узла контроллера. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**.

   e. В поле **Порт** введите номер базового порта узла контроллера. Диапазон значений: от 1 до 65 535. Значение по умолчанию: `6653`. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**.

      Вместе с базовым портом узла контроллера автоматически указываются порты с тремя следующими по порядку номерами. Например, если вы вводите номер базового порта `6653`, автоматически указываются порты 6654, 6655 и 6656.

   > Вам нужно перезагрузить устройство CPE после изменения IP-адресов и номеров TCP-портов узлов контроллера на интерфейсе SD-WAN с типом WAN, чтобы изменения вступили в силу.

   Вы можете изменить IP-адреса и номера TCP-портов узлов контроллера при настройке узлов контроллера экземпляра SD-WAN. В этом случае IP-адреса и номера TCP-портов узлов контроллера автоматически изменятся на всех устройствах CPE, которые добавлены экземпляру SD-WAN. IP-адреса и номера TCP-портов, указанные на отдельном интерфейсе SD-WAN с типом WAN, являются более приоритетными по отношению к IP-адресам и номерам TCP-портов, указанным при настройке узлов контроллера экземпляра SD-WAN.

10. При необходимости включите функцию FEC на вкладке **Параметры соединений**.

11. Нажмите на кнопку **Создать**.

    Интерфейс SD-WAN с типом WAN будет создан и отобразится в таблице.

12. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение интерфейса SD-WAN

Вы можете изменить интерфейс SD-WAN в шаблоне CPE или на устройстве CPE. Вы не можете изменить имя интерфейса SD-WAN. При изменении интерфейса SD-WAN с типом LAN вы можете только указать максимальную скорость и настроить очереди трафика. Интерфейс SD-WAN, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить интерфейс SD-WAN:

1. Перейдите к изменению интерфейса SD-WAN одним из следующих способов:

   - Если вы хотите изменить интерфейс SD-WAN в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **SD-WAN → Интерфейсы**.

   - Если вы хотите изменить интерфейс SD-WAN на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **SD-WAN → Интерфейсы**. Если вы хотите изменить интерфейс SD-WAN, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с интерфейсом SD-WAN.

   Отобразится таблица интерфейсов SD-WAN.

2. Нажмите на кнопку **Изменить** рядом с интерфейсом SD-WAN, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры интерфейса SD-WAN. Описание параметров см. в инструкции по созданию интерфейса с типом WAN.

4. Нажмите на кнопку **Сохранить**.

   Интерфейс SD-WAN будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Выключение и включение интерфейса SD-WAN

Вы можете выключить или включить интерфейс SD-WAN в шаблоне CPE или на устройстве CPE. Интерфейс SD-WAN, выключенный или включенный в шаблоне CPE, автоматически выключается или включается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы выключить или включить интерфейс SD-WAN:

1. Перейдите к выключению или включению интерфейса SD-WAN одним из следующих способов:

   - Если вы хотите выключить или включить интерфейс SD-WAN в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **SD-WAN → Интерфейсы**.

   - Если вы хотите выключить или включить интерфейс SD-WAN на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **SD-WAN → Интерфейсы**. Если вы хотите выключить или включить интерфейс SD-WAN, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с интерфейсом SD-WAN.

   Отобразится таблица интерфейсов SD-WAN.

2. Нажмите на кнопку **Выключить** или **Включить** рядом с интерфейсом SD-WAN, который вы хотите выключить или включить.

   Интерфейс SD-WAN будет выключен или включен и обновится в таблице.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление интерфейса SD-WAN с типом WAN

Вы можете удалить интерфейс SD-WAN с типом WAN в шаблоне CPE или на устройстве CPE. Интерфейс SD-WAN с типом WAN, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете удалить на устройстве CPE интерфейс SD-WAN, унаследованный из шаблона CPE, а также удалить интерфейс SD-WAN с типом LAN.

Удаленные интерфейсы SD-WAN с типом WAN невозможно восстановить.

Чтобы удалить интерфейс SD-WAN с типом WAN:

1. Перейдите к удалению интерфейса SD-WAN с типом WAN одним из следующих способов:

   - Если вы хотите удалить интерфейс SD-WAN с типом WAN в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **SD-WAN → Интерфейсы**.

   - Если вы хотите удалить интерфейс SD-WAN с типом WAN на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

2. Нажмите на кнопку **Удалить** рядом с интерфейсом SD-WAN с типом WAN, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Интерфейс SD-WAN с типом WAN будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с сервисными интерфейсами

Сервисные интерфейсы ссылаются на OpenFlow-порты и используются для подключения устройства CPE к транспортным сервисам. Сервисный интерфейс не может ссылаться на OpenFlow-порт, на который уже ссылается интерфейс SD-WAN с типом WAN.

При необходимости фильтровать пакеты трафика на сервисном интерфейсе вы можете создать ACL-интерфейс (Access Control List), ссылающийся на сервисный интерфейс. ACL-интерфейс применяет к сервисному интерфейсу указанный фильтр трафика. На один сервисный интерфейс могут ссылаться не более четырех ACL-интерфейсов.

Для просмотра таблицы сервисных интерфейсов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **Сервисные интерфейсы**. Информация о сервисных интерфейсах отображается в следующих столбцах таблицы:

- **Порт** – номер OpenFlow-порта, на который ссылается сервисный интерфейс.
- **Тип** – тип классификации трафика на сервисном интерфейсе:
  - **Access**.
  - **VLAN**.
  - **Q-in-Q**.
  - **ACL**.
- **Описание** – краткое описание сервисного интерфейса.
- **VLAN** – внешняя метка VLAN сервисного интерфейса. Значение в этом столбце отображается только для сервисных интерфейсов с типами классификации трафика **VLAN** и **Q-in-Q**.
- **Внутренний VLAN** – внутренняя метка VLAN сервисного интерфейса. Значение в этом столбце отображается только для сервисных интерфейсов с типом классификации трафика **Q-in-Q**.
- **Фильтр** – фильтр трафика для ACL-интерфейса. Значение в этом столбце отображается только для сервисных интерфейсов с типом классификации трафика **ACL**.
- **Имя** – информация о сервисном интерфейсе:
  - имя и идентификатор DPID устройства CPE, на котором создан сервисный интерфейс;
  - номер OpenFlow-порта, на который ссылается сервисный интерфейс.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание сервисного интерфейса

Чтобы создать сервисный интерфейс:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сервисные интерфейсы**.

   Отобразится таблица сервисных интерфейсов и ACL-интерфейсов.

4. В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-порт, на который ссылается сервисный интерфейс.

5. Нажмите на кнопку **Создать сервисный интерфейс**.

6. В открывшемся окне в раскрывающемся списке **Тип** выберите тип классификации трафика на сервисном интерфейсе:

   - **Access**. Это значение выбрано по умолчанию.
   - **VLAN**. При выборе этого значения в поле **VLAN ID** введите внешнюю метку VLAN сервисного интерфейса. Диапазон значений: от 1 до 4094.
   - **Q-in-Q**. При выборе этого значения выполните следующие действия:

     a. В поле **VLAN ID** введите внешнюю метку VLAN сервисного интерфейса. Диапазон значений: от 1 до 4094.

     b. В поле **Внутренний VLAN ID** введите внутреннюю метку VLAN сервисного интерфейса. Диапазон значений: от 1 до 4094.

   - **ACL** – используется при создании ACL-интерфейса.

7. При необходимости в поле **Описание** введите краткое описание сервисного интерфейса.

8. Нажмите на кнопку **Создать**.

Сервисный интерфейс будет создан и отобразится в таблице.

Создание ACL-интерфейса

Чтобы создать ACL-интерфейс:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сервисные интерфейсы**.

   Отобразится таблица сервисных интерфейсов и ACL-интерфейсов.

4. В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-порт, на который ссылается созданный сервисный интерфейс.

5. Нажмите на кнопку **Создать сервисный интерфейс**.

6. В открывшемся окне в раскрывающемся списке **Тип** выберите **ACL**.

7. В раскрывающемся списке **Сервисный интерфейс** выберите сервисный интерфейс, на который ссылается ACL-интерфейс.

8. В раскрывающемся списке **Фильтр трафика** выберите созданный фильтр трафика для ACL-интерфейса. Вы можете использовать один фильтр трафика для нескольких ACL-интерфейсов.

9. В раскрывающемся списке **Порядок** выберите порядковый номер ACL-интерфейса. В первую очередь трафик направляется в ACL-интерфейс с наименьшим значением порядкового номера. Если фильтр, используемый в ACL-интерфейсе, не забирает трафик, трафик направляется во второй по порядку ACL-интерфейс и так далее.

   Диапазон значений: от 1 до 4. Два ACL-интерфейса с одинаковым порядковым номером не могут ссылаться на один сервисный интерфейс.

10. При необходимости в поле **Описание** введите краткое описание ACL-интерфейса.

11. Нажмите на кнопку **Создать**.

ACL-интерфейс будет создан и отобразится в таблице.

Просмотр использования сервисного интерфейса и ACL-интерфейса

При необходимости вы можете посмотреть, какие транспортные сервисы используют сервисный интерфейс или ACL-интерфейс. Например, если сервисный интерфейс или ACL-интерфейс используется, его невозможно удалить.

Чтобы посмотреть, используется ли сервисный интерфейс или ACL-интерфейс:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сервисные интерфейсы**.

   Отобразится таблица сервисных интерфейсов и ACL-интерфейсов.

4. Нажмите на кнопку **Управление** → **Показать использование** рядом с сервисным интерфейсом или ACL-интерфейсом, использование которого вы хотите посмотреть.

Откроется окно с таблицей транспортных сервисов, использующих сервисный интерфейс или ACL-интерфейс.

Удаление сервисного интерфейса и ACL-интерфейса

Вы не можете удалить сервисный интерфейс или ACL-интерфейс, если он используется хотя бы одним транспортным сервисом. Для удаления сервисного интерфейса или ACL-интерфейса, который используется транспортными сервисами, вам нужно сначала убрать сервисный интерфейс или ACL-интерфейс из параметров транспортных сервисов. Вы можете посмотреть, какие транспортные сервисы используют сервисный интерфейс или ACL-интерфейс.

Удаленные сервисные интерфейсы и ACL-интерфейсы невозможно восстановить.

Чтобы удалить сервисный интерфейс или ACL-интерфейс:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сервисные интерфейсы**.

   Отобразится таблица сервисных интерфейсов и ACL-интерфейсов.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с сервисным интерфейсом или ACL-интерфейсом, который вы хотите удалить.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Сервисный интерфейс или ACL-интерфейс будет удален и перестанет отображаться в таблице.

Работа с группами OpenFlow-портов

OpenFlow-порты – это интерфейсы наложенной SDN-сети, которые создаются автоматически одновременно с интерфейсами SD-WAN. Контроллер использует OpenFlow-порты, чтобы управлять трафиком сети. Вы можете создавать сервисные интерфейсы и UNI, которые ссылаются на OpenFlow-порты.

OpenFlow-порты можно объединить в группы OpenFlow-портов и использовать их при создании транспортных сервисов P2M и M2M. Когда вы добавляете группу OpenFlow-портов в транспортный сервис, автоматически создаются сервисные интерфейсы, ссылающиеся на OpenFlow-порты, после чего сервисные интерфейсы добавляются в транспортный сервис. Использование групп OpenFlow-портов избавляет вас от необходимости вручную создавать сервисные интерфейсы и добавлять их в транспортные сервисы.

Для просмотра таблицы групп OpenFlow-портов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление → Параметры развертывания** рядом с контроллером и перейти в раздел **Группы OpenFlow-портов**. Информация о группах OpenFlow-портов отображается в следующих столбцах таблицы:

- **Имя** – имя группы OpenFlow-портов.
- **OpenFlow-порты** – OpenFlow-порты, которые были добавлены в группу OpenFlow-портов.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание группы OpenFlow-портов

Чтобы создать группу OpenFlow-портов:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Группы OpenFlow-портов**.

   Отобразится таблица групп OpenFlow-портов.

4. В верхней части страницы нажмите на кнопку **+ Группа OpenFlow-портов**.

5. В открывшемся окне в поле **Имя** введите имя группы OpenFlow-портов.

6. В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-порт, который вы хотите добавить в группу OpenFlow-портов.

   Вы можете добавить несколько OpenFlow-портов и удалить OpenFlow-порты. Для удаления OpenFlow-порта нажмите рядом с ним на кнопку **Удалить**.

7. Нажмите на кнопку **Создать**.

Группа OpenFlow-портов будет создана и отобразится в таблице.

Изменение группы OpenFlow-портов

Чтобы изменить группу OpenFlow-портов:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Группы OpenFlow-портов**.

   Отобразится таблица групп OpenFlow-портов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с группой OpenFlow-портов, которую вы хотите изменить.

5. В открывшемся окне при необходимости измените имя группы OpenFlow-портов и добавьте или удалите OpenFlow-порты.

6. Нажмите на кнопку **Сохранить**.

Группа OpenFlow-портов будет изменена и обновится в таблице.

Удаление группы OpenFlow-портов

Удаленные группы OpenFlow-портов невозможно восстановить.

Чтобы удалить группу OpenFlow-портов:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Группы OpenFlow-портов**.

   Отобразится таблица групп OpenFlow-портов.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с группой OpenFlow-портов, которую вы хотите удалить.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Группа OpenFlow-портов будет удалена и перестанет отображаться в таблице.

Настройка UNI для подключения устройств CPE к сетевым сервисам

UNI ссылаются на OpenFlow-порты и используются для подключения устройства CPE к сетевым сервисам. UNI не может ссылаться на OpenFlow-порт, на который уже ссылается интерфейс SD-WAN с типом WAN.

Для централизованной настройки UNI на устройствах CPE используются шаблоны UNI. Вам нужно создать UNI в шаблоне UNI, после чего указать шаблон UNI при добавлении или ручной регистрации устройства CPE, чтобы не создавать UNI на каждом отдельном устройстве CPE. Если вы измените UNI в шаблоне UNI, UNI автоматически изменяется на всех устройствах CPE, которые используют шаблон UNI.

При создании UNI для него автоматически создается сервисный интерфейс.

Работа с шаблонами UNI

Вы можете посмотреть таблицу шаблонов UNI в разделе **SD-WAN → Шаблоны UNI**. Информация о шаблонах UNI отображается в следующих столбцах таблицы:

- **ID** – идентификатор шаблона UNI.
- **Имя** – имя шаблона UNI.
- **Используется** – шаблон UNI используется устройствами CPE:
  - **Да**.
  - **Нет**.
- **Изменено** – дата и время последнего изменения параметров шаблона UNI.
- **Пользователь** – имя пользователя, который создал шаблон UNI.
- **Владелец** – тенант, к которому относится шаблон UNI.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Параметры шаблона UNI можно настроить на следующих вкладках:

- **Информация** – основная информация о шаблоне UNI. Вы можете изменить имя шаблона UNI в поле **Имя**.
- **UNI** – UNI, которые были созданы в шаблоне UNI.

Создание шаблона UNI

Чтобы создать шаблон UNI:

1. В меню перейдите в подраздел **SD-WAN → Шаблоны UNI**.

   Отобразится таблица шаблонов UNI.

2. В верхней части страницы нажмите на кнопку **+ Шаблон UNI**.

3. В открывшемся окне введите имя шаблона UNI.

4. Нажмите на кнопку **Создать**.

Шаблон UNI будет создан и отобразится в таблице.

Вам нужно настроить созданный шаблон UNI. Более подробно о работе с шаблонами UNI см. в разделе Работа с шаблонами UNI.

Удаление шаблона UNI

Удаленные шаблоны UNI невозможно восстановить.

Чтобы удалить шаблон UNI:

1. В меню перейдите в подраздел **SD-WAN → Шаблоны UNI**.

   Отобразится таблица шаблонов UNI.

2. Нажмите на шаблон UNI, который вы хотите удалить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона UNI и тенант, которому шаблон UNI назначен.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Шаблон UNI будет удален и перестанет отображаться в таблице.

Работа с UNI

Работа с UNI в шаблоне UNI

Для просмотра таблицы UNI в шаблоне UNI вам нужно в меню перейти в раздел **SD-WAN → Шаблоны UNI**, нажать на шаблон UNI и выбрать вкладку **UNI**. Информация о UNI отображается в следующих столбцах таблицы:

- **Имя** – имя UNI.
- **OpenFlow-порт** – номер OpenFlow-порта, на который ссылается UNI.
- **Классификация** – тип классификации трафика на UNI:
  - **Access**.
  - **VLAN**.
  - **Q-in-Q**.
- **Действия** – действия, которые можно выполнить с UNI.

Работа с UNI на устройстве CPE

Для просмотра списка UNI на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **UNI**.

Создание UNI

Вы можете создать UNI в шаблоне UNI или на устройстве CPE. UNI, созданный в шаблоне UNI, автоматически создается на всех устройствах CPE, которые используют шаблон UNI.

Чтобы создать UNI:

1. Перейдите к созданию UNI одним из следующих способов:
   - Если вы хотите создать UNI в шаблоне UNI, в меню перейдите в раздел **SD-WAN → Шаблоны UNI**, нажмите на шаблон UNI и выберите вкладку **UNI**.
   - Если вы хотите создать UNI на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **UNI**.

   Отобразится таблица или список UNI.
2. Нажмите на кнопку **+ UNI**.
3. В открывшемся окне в поле **Имя** введите имя UNI.

4. Укажите OpenFlow-порт, на который ссылается UNI, одним из следующих способов:

   - Если вы создаете UNI в шаблоне UNI, в поле **OpenFlow-порт** введите номер OpenFlow-порта.
   - Если вы создаете UNI на устройстве CPE, в раскрывающемся списке **Порт** выберите OpenFlow-порт.

5. В раскрывающемся списке **Классификация** выберите тип классификации трафика на UNI:

   - **Access**. Это значение выбрано по умолчанию.
   - **VLAN**. При выборе этого значения в поле **VLAN ID** введите внешнюю метку VLAN UNI. Диапазон значений: от 1 до 4094.
   - **Q-in-Q**. При выборе этого значения выполните следующие действия:

     a. В поле **VLAN ID** введите внешнюю метку VLAN UNI. Диапазон значений: от 1 до 4094.

     b. В поле **Внутренний VLAN ID** введите внутреннюю метку VLAN UNI. Диапазон значений: от 1 до 4094.

6. Если вы создаете UNI на устройстве CPE, в раскрывающемся списке **QoS** выберите созданное правило качества обслуживания для UNI.

7. Нажмите на кнопку **Создать**.

   UNI будет создан и отобразится в таблице или списке.

8. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона UNI или устройства CPE.

Просмотр использования UNI

При необходимости вы можете посмотреть, какие сетевые сервисы используют UNI на устройстве CPE. Например, если UNI используется, его невозможно удалить.

Чтобы посмотреть, используется ли UNI:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите посмотреть использование UNI.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **UNI**.

   Отобразится список UNI.

4. Нажмите на кнопку **Управление → Показать использование** рядом с UNI, использование которого вы хотите посмотреть.

Откроется окно с таблицей сетевых сервисов, использующих UNI.

Изменение UNI

Вы можете изменить UNI в шаблоне UNI. UNI, измененный в шаблоне UNI, автоматически изменяется на всех устройствах CPE, которые используют шаблон UNI.

Чтобы изменить UNI:

1. В меню перейдите в подраздел **SD-WAN → Шаблоны UNI**.

   Отобразится таблица шаблонов UNI.

2. Нажмите на шаблон UNI, в котором вы хотите изменить UNI.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона UNI и тенант, которому шаблон UNI назначен.

3. Выберите вкладку **UNI**.

   Отобразится таблица UNI.

4. Нажмите на кнопку **Изменить** рядом с UNI, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры UNI. Описание параметров см. в инструкции по созданию UNI.

6. Нажмите на кнопку **Сохранить**.

   UNI будет изменен и обновится в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона UNI.

Удаление UNI

Вы можете удалить UNI в шаблоне UNI или на устройстве CPE. UNI, удаленный в шаблоне UNI, автоматически удаляется на всех устройствах CPE, которые используют шаблон UNI.

Удаленные UNI невозможно восстановить.

Удаление UNI в шаблоне UNI

Чтобы удалить UNI в шаблоне UNI:

1. В меню перейдите в подраздел **SD-WAN → Шаблоны UNI**.

   Отобразится таблица шаблонов UNI.

2. Нажмите на шаблон UNI, в котором вы хотите удалить UNI.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона UNI и тенант, которому шаблон UNI назначен.

3. Выберите вкладку **UNI**.

   Отобразится таблица UNI.

4. Нажмите на кнопку **Удалить** рядом с UNI, который вы хотите удалить.

   UNI будет удален и перестанет отображаться в таблице.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона UNI.

Удаление UNI на устройстве CPE

Вы не можете удалить UNI, если он используется хотя бы одним сетевым сервисом. Для удаления UNI, который используется сетевыми сервисами, вам нужно сначала удалить UNI из топологии сетевых сервисов. Вы можете посмотреть, какие сетевые сервисы используют UNI.

Чтобы удалить UNI на устройстве CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите удалить UNI.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **UNI**.

   Отобразится список UNI.

4. Нажмите на кнопку **Управление → Удалить** рядом с UNI, который вы хотите удалить.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   UNI будет удален и перестанет отображаться в таблице.

6. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Добавление статического маршрута

Помимо динамического обмена маршрутами между устройствами CPE и внешними сетевыми устройствами по протоколам BGP и OSPF, Kaspersky SD-WAN поддерживает статические IPv4-маршруты. Вы можете добавить статический маршрут в шаблоне CPE или на устройстве CPE. Статический маршрут, добавленный в шаблоне CPE, автоматически добавляется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы добавить статический маршрут:

1. Перейдите к добавлению статического маршрута одним из следующих способов:

   - Если вы хотите добавить статический маршрут в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Статические маршруты**.

   - Если вы хотите добавить статический маршрут на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Статические маршруты** и установите флажок **Переопределить**.

   Отобразится таблица статических маршрутов.

2. Нажмите на кнопку **+ Добавить**.

3. В раскрывающемся списке **VRF** выберите виртуальную таблицу маршрутизации. Этот параметр является обязательным.

4. В раскрывающемся списке **Интерфейс** выберите созданный сетевой интерфейс источника статического маршрута. Этот параметр является обязательным, если в качестве виртуальной таблицы маршрутизации выбран VRF main/254.

   Список доступных для выбора интерфейсов формируется на основе выбранного на предыдущем шаге VRF.: Вы можете выбрать только те интерфейсы, которые принадлежат выбранному VRF, отличному от main/254, и любые интерфейсы из VRF main/254.

5. В поле **Назначение** введите IPv4-адрес назначения статического маршрута.

6. При необходимости в поле **IPv4-маска** введите IPv4-адрес подсети назначения статического маршрута.

7. В поле **Шлюз** введите IPv4-адрес шлюза статического маршрута.

   Поле недоступно для заполнения, если в списке **Тип** выбран типа маршрута **blackhole**.

8. В поле **Метрика** введите метрику статического маршрута. Значение по умолчанию: `0`.

   Поле недоступно для заполнения, если в списке **Тип** выбран тип маршрута **blackhole** или если статический маршрут создается в виртуальной таблиц маршрутизации, отличной от VRF main/254.

9. В поле **MTU** введите значение MTU статического маршрута.

   Поле недоступно для заполнения, если в списке **Тип** выбран тип маршрута **blackhole** или если статический маршрут создается в виртуальной таблице маршрутизации, отличной от VRF main/254.

10. В поле **AD** введите административное расстояние для статического маршрута.

    Поле недоступно для заполнения, если статический маршрут создается в VRF main/254. Значение по умолчанию: `1`.

    Таблица соответствия административных расстояний и протоколов маршрутизации приведена в соответствующей статье.

11. В раскрывающемся списке **Тип** выберите тип статического маршрута:

    - **unicast**. Это значение выбрано по умолчанию.
    - **local**. Доступно только для VRF main/254).
    - **broadcast**. Доступно только для VRF main/254).
    - **multicast**. Доступно только для VRF main/254).
    - **unreachable**. Доступно только для VRF main/254).
    - **prohibit**. Доступно только для VRF main/254).
    - **anycast**. Доступно только для VRF main/254).
    - **blackhole**.

      При выборе типа маршрута **blackhole** становятся недоступными для заполнения поля **Шлюз**, **Метрика** и **MTU**.

      > Если вам нужно использовать blackhole-маршрут по умолчанию 0.0.0.0/0 для изоляции маршрутов между VRF, добавьте его для соответствующего VRF на вкладке **VRF** в разделе **SD-WAN → Шаблоны CPE** или **SD-WAN → CPE**, выбрав **Добавить blackhole-маршрут**. При попытке добавить такой маршрут на вкладке **Статические маршруты** отобразится сообщение об ошибке.

    Статический маршрут будет добавлен и отобразится в таблице. Вы можете добавить несколько статических маршрутов и удалить статические маршруты. Для удаления статического маршрута нажмите рядом с ним на значок удаления ✕.

12. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Таблица соответствия административных расстояний для протоколов маршрутизации

Протокол	Расстояние
System	0
Kernel	0
Connect	0
Static	1
NHRP	10
EBGP	20
EIGRP	90
BABEL	100
OSPF	110
ISIS	115

OPENFABRIC	115
RIP	120
Table	150
SHARP	150
IBGP	200
PBR	200

Фильтрация маршрутов и пакетов трафика

Вы можете использовать следующие механизмы для фильтрации маршрутов при работе с протоколами BGP и OSPF, а также для фильтрации пакетов трафика при работе с протоколом PIM:

- Списки управления доступом (англ. Access Control Lists, ACL) – разрешают или запрещают указанные IPv4-префиксы.
- Списки префиксов (англ. prefix lists) – расширенная версия списков управления доступом. Дополнительно разрешают или запрещают IPv4-префиксы с указанным диапазоном длины префикса. Вы можете использовать списки префиксов в картах маршрутизации.
- Списки community (англ. community lists) – управление префиксами на основе маркировок. Вы можете использовать списки community в картах маршрутизации.
- Карты маршрутизации (англ. route maps) –расширенная версия списков префиксов. Дополнительно изменяют значения атрибутов.

Вы можете создавать правила в списках управления доступом, списках префиксов, списках community и картах маршрутизации. Каждое правило имеет порядковый номер. Первым к IPv4-префиксу применяется правило с наименьшим значением порядкового номера. Если ни одно из правил не может быть применено, IPv4-префикс запрещается.

Описанные далее механизмы фильтрафии маршрутов могут использоваться в разных сценариях маршрутизации, например, для того, чтобы:

- разделить трафик по каналам, упростить политику распределения нагрузки и аварийного переключения;
- для разных подсетей (или приложений) направлять трафик в заранее определенный канал;
- направить трафик к определенным корпоративным сервисам (например, дата-центрам) через более быстрый/дорогой канал, а остальной трафик – через дешевый канал;
- сделать один из каналов менее привлекательным для внешних провайдеров, добавляя к его маршрутам более длинный AS-Path.

Работа со списками управления доступом (ACLs)

Вы можете посмотреть таблицу списков управления доступом в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы списков управления доступом в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **Фильтры маршрутов → Списки управления доступом**.
- Для просмотра таблицы списков управления доступом на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Фильтры маршрутов → Списки управления доступом**.

Информация о списках управления доступом отображается в следующих столбцах таблицы:

- **Имя** – имя списка управления доступом.
- **Унаследовано** – список управления доступом унаследован из шаблона CPE:
  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.
- **Порядок** – порядковый номер правила в списке управления доступом. Список управления доступом первым применяет к IPv4-префиксу правило с наименьшим значением порядкового номера.
- **Сеть** – IPv4-префикс, к которому список управления доступом применяет правило.
- **Действие** – действие, которое правило выполняет с IPv4-префиксом:
  - **Разрешить** – разрешить IPv4-префикс.
  - **Отклонить** – запретить IPv4-префикс.
- **Управление** – действия, которые можно выполнить со списком управления доступом.

Создание списка управления доступом

Вы можете создать список управления доступом в шаблоне CPE или на устройстве CPE. Список управления доступом, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать список управления доступом:

1. Перейдите к созданию списка управления доступом одним из следующих способов:

   - Если вы хотите создать список управления доступом в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Фильтры маршрутов → Списки управления доступом**.

   - Если вы хотите создать список управления доступом на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Фильтры маршрутов → Списки управления доступом** и установите флажок **Переопределить**.

   Отобразится таблица списков управления доступом.

2. Нажмите на кнопку **+ Список управления доступом**.

3. В открывшемся окне в поле **Имя** введите имя списка управления доступом. Максимальная длина имени: 50 символов. Не используйте пробелы в этом поле.

4. Создайте правило в списке управления доступом:

   a. Нажмите на кнопку **+ Правило**.

   b. В поле **Порядок** введите порядковый номер правила. Список управления доступом первым применяет к IPv4-префиксу правило с наименьшим значением порядкового номера. Диапазон значений: от 1 до 4 294 967 295.

   c. В раскрывающемся списке **Сеть** выберите тип правила:

      - **Любая сеть** – правило, разрешающее или запрещающее любые IPv4-префиксы.

      - **IP/маска** – правило, разрешающее или запрещающее указанный IPv4-префикс. Это значение выбрано по умолчанию. При выборе этого значения в отобразившемся поле введите IPv4-префикс.

   d. В раскрывающемся списке **Действие** выберите действие, которое правило выполняет с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Это значение выбрано по умолчанию.

      - **Отклонить** – запретить IPv4-префикс.

   Правило будет создано. Вы можете создать несколько правил и удалить правила. Для удаления правила нажмите рядом с ним на значок удаления ✕.

5. Нажмите на кнопку **Создать**.

   Список управления доступом будет создан и отобразится в таблице.

6. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение списка управления доступом

Вы можете изменить список управления доступом в шаблоне CPE или на устройстве CPE. Список управления доступом, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить список управления доступом:

1. Перейдите к изменению списка управления доступом одним из следующих способов:

   - Если вы хотите изменить список управления доступом в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Фильтры маршрутов → Списки управления доступом**.

   - Если вы хотите изменить список управления доступом на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Фильтры маршрутов → Списки управления доступом** и установите флажок **Переопределить**.

   Отобразится таблица списков управления доступом.

2. Нажмите на кнопку **Изменить** рядом со списком управления доступом, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры списка управления доступом. Описание параметров см. в инструкции по созданию списка управления доступом.

4. Нажмите на кнопку **Сохранить**.

   Список управления доступом будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление списка управления доступом

Вы можете удалить список управления доступом в шаблоне CPE или на устройстве CPE. Список управления доступом, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE.

Удаленные списки управления доступом невозможно восстановить.

Чтобы удалить список управления доступом:

1. Перейдите к удалению списка управления доступом одним из следующих способов:

   - Если вы хотите удалить список управления доступом в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Фильтры маршрутов → Списки управления доступом**.

   - Если вы хотите удалить список управления доступом на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Фильтры маршрутов → Списки управления доступом** и установите флажок **Переопределить**.

   Отобразится таблица списков управления доступом.

2. Нажмите на кнопку **Удалить** рядом со списком управления доступом, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Список управления доступом будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа со списками префиксов (prefix lists)

Вы можете посмотреть таблицу списков префиксов в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы списков префиксов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **Фильтры маршрутов → Списки префиксов**.

- Для просмотра таблицы списков префиксов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Фильтры маршрутов → Списки префиксов**.

Информация о списках префиксов отображается в следующих столбцах таблицы:

- **Имя** – имя списка префиксов.

- **Унаследовано** – список префиксов унаследован из шаблона CPE:

  - **Да**.

  - **Нет**.

  Этот столбец отображается только на устройстве CPE.

- **Порядок** – порядковый номер правила в списке префиксов. Список префиксов первым применяет к IPv4-префиксу правило с наименьшим значением порядкового номера.

- **Сеть** – IPv4-префикс, к которым список префиксов применяет правило.

- **Действие** – действие, которое правило выполняет с IPv4-префиксом:
  - **Разрешить** – разрешить IPv4-префикс.
  - **Отклонить** – запретить IPv4-префикс.
- **Больше или равно** – начальное значение диапазона длины префикса, к которому список префиксов применяет правило.
- **Меньше или равно** – конечное значение диапазона длины префикса, к которому список префиксов применяет правило.
- **Управление** – действия, которые можно выполнить со списком префиксов.

Создание списка префиксов

Вы можете создать список префиксов в шаблоне CPE или на устройстве CPE. Список префиксов, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать список префиксов:

1. Перейдите к созданию списка префиксов одним из следующих способов:
   - Если вы хотите создать список префиксов в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Фильтры маршрутов → Списки префиксов**.
   - Если вы хотите создать список префиксов на устройстве CPE, в меню перейдите в раздел **SD-WAN** , нажмите на устройство CPE, выберите вкладку **Фильтры маршрутов → Списки префиксов** и установите флажок **Переопределить**.

   Отобразится таблица списков префиксов.
2. Нажмите на кнопку **+ Список префиксов**.
3. В открывшемся окне в поле **Имя** введите имя списка префиксов. Максимальная длина имени: 50 символов. Не используйте пробелы в этом поле.

4. Создайте правило в списке префиксов:

   a. Нажмите на кнопку **+ Правило**.

   b. В поле **Порядок** введите порядковый номер правила. Список префиксов первым применяет к IPv4-префиксу правило с наименьшим значением порядкового номера. Диапазон значений: от 1 до 4 294 967 295.

   c. В раскрывающемся списке **Сеть** выберите тип правила:

      - **Любая сеть** – правило, разрешающее или запрещающее любые IPv4-префиксы.
      - **IP/маска** – правило, разрешающее или запрещающее указанный IPv4-префикс. Это значение выбрано по умолчанию. При выборе этого значения в отобразившемся поле введите IPv4-префикс.

   d. В раскрывающемся списке **Действие** выберите действие, которое правило выполняет с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Это значение выбрано по умолчанию.
      - **Отклонить** – запретить IPv4-префикс.

   e. В поле **Больше или равно** введите начальное значение диапазона длины префикса, к которому список префиксов применяет правило. Диапазон значений: от 0 до 32.

   f. В поле **Меньше или равно** введите конечное значение диапазона длины префикса, к которому список префиксов применяет правило. Диапазон значений: от 0 до 32.

   Правило будет создано. Вы можете создать несколько правил и удалить правила. Для удаления правила нажмите рядом с ним на значок удаления ✕.

5. Нажмите на кнопку **Создать**.

   Список префиксов будет создан и отобразится в таблице.

6. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение списка префиксов

Вы можете изменить список префиксов в шаблоне CPE или на устройстве CPE. Список префиксов, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить список префиксов:

1. Перейдите к изменению списка префиксов одним из следующих способов:

   - Если вы хотите изменить список префиксов в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Фильтры маршрутов** → **Списки префиксов**.

   - Если вы хотите изменить список префиксов на устройстве CPE, в меню перейдите в раздел **SD-WAN** , нажмите на устройство CPE, выберите вкладку **Фильтры маршрутов** → **Списки префиксов** и установите флажок **Переопределить**.

   Отобразится таблица списков префиксов.

2. Нажмите на кнопку **Изменить** рядом со списком префиксов, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры списка префиксов. Описание параметров см. в инструкции по созданию списка префиксов.

4. Нажмите на кнопку **Сохранить**.

   Список префиксов будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление списка префиксов

Вы можете удалить список префиксов в шаблоне CPE или на устройстве CPE. Список префиксов, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE.

Удаленные списки префиксов невозможно восстановить.

Чтобы удалить список префиксов:

1. Перейдите к удалению списка префиксов одним из следующих способов:

   - Если вы хотите удалить список префиксов в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Фильтры маршрутов** → **Списки префиксов**.

   - Если вы хотите удалить список префиксов на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Фильтры маршрутов** → **Списки префиксов** и установите флажок **Переопределить**.

   Отобразится таблица списков префиксов.

2. Нажмите на кнопку **Удалить** рядом со списком префиксов, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Список префиксов будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа со списками community

Вы можете посмотреть таблицу списков community в шаблоне CPE и на устройстве CPE:

Для просмотра таблицы списков community в шаблоне CPE вам нужно в меню перейти в раздел SD-WAN → Шаблоны CPE, нажать на шаблон CPE и выбрать вкладку Маршрутизация → Фильтры маршрутов → Списки community

Для просмотра таблицы списков community на устройстве CPE вам нужно в меню перейти в раздел SD-WAN → CPE, нажать на устройство CPE и выбрать вкладку Маршрутизация → Фильтры маршрутов → Списки community

Информация о списках community отображается в следующих столбцах таблицы:

Имя – имя списка community

Переопределить:

Да – параметры списка community уникальны и не наследуются из шаблона.

Нет – параметры списка community наследуются из шаблона.

Этот столбец отображается только на устройстве CPE. Вы можете изменить значение этого столбца для каждого списка community непосредственно в таблице.

Унаследовано – список community унаследован из шаблона CPE:

Да

Нет

Этот столбец также отображается только на устройстве CPE.

Тип – тип списка community – стандартный или расширенный.

Порядок - порядковый номер правила в списке community. Список community первым применяет правило с наименьшим значением порядкового номера.

Действие - действие, которое правило выполняет с значением community:

Разрешить – разрешить community

Отклонить – запретить community

Значение – маркировка префикса IPv4, позволяющая применять к нему политики.

Создание списка community -

Вы можете создать список community в шаблоне CPE или на устройстве CPE.

Перейдите к созданию списка community одним из следующих способов:

Если вы хотите создать список community в шаблоне CPE, в меню перейдите в раздел SD-WAN → Шаблоны CPE → Маршрутизация → Фильтры маршрутов → Списки community и в верхней части страницы нажмите на кнопку + Добавить.

Если вы хотите создать список community на устройстве CPE, в меню перейдите в раздел SD-WAN → CPE, нажмите на устройство CPE, выберите вкладку Маршрутизация → Фильтры маршрутов → Списки community и в верхней части страницы нажмите на кнопку + Добавить.

Отобразится таблица списков community.

В открывшемся окне в поле Имя введите имя списка community. Максимальная длина имени: 50 символов.

Обратите внимание, имя списка community является уникальным в рамках тенанта.

В поле Тип нужно выбрать между стандартным (точное совпадение значения) и расширенным (совпадение на основе регулярного выражения) типом community.

Теперь с помощью кнопки + Добавить можно добавлять записи community в список.

Поле Порядок записей community автоматически формирует номера с шагом 10, начиная со значения 10. Порядковый номер (и порядок применения записей) можно изменять с помощью элемента меню «Счетчик».

Далее выберите Действие: Отклонить или Разрешить для создаваемой записи community.

Стандартный тип community

Далее можно ввести значения community, выбрав их из выпадающего перечня либо введя их в виде списка текстовых значений. Также community может быть задана числовым значением вида <число от 0 до 65535>: <число от 0 до 65535>. Возможны комбинации из значений, введенных пользователем и предустановленных значений.

Расширенный тип community

Далее можно ввести значения community в виде регулярного выражения.

Если вы хотите удалить запись community из списка, выделите запись (поставьте «галочку» спереди записи) и нажмите кнопку «Удалить».

Теперь созданный список community можно использовать в match и/или set инструкции внутри route-map для манипуляции BGP префиксами (ссылка на раздел Работа с картами маршрутизации (route maps)).

Изменение списка community -

Чтобы изменить требуемый список community, выделите список (поставьте «галочку» спереди списка) и нажмите кнопку «Изменить», либо нажмите на имя списка community.

Теперь Вы можете добавить новые или удалить существующие элементы списка community.

Удаление списка community -

Чтобы удалить список community, выделите соответствующий список (поставьте «галочку» спереди списка) и нажмите кнопку «Удалить». За один раз можно удалить только один список.

Создание списка community

Вы можете создавать списки community в шаблоне CPE или на устройстве CPE. Списки community, созданные в шаблоне CPE, автоматически создаются на всех устройствах CPE, которые используют этот шаблон CPE.

Чтобы создать список community:

1. Перейдите к созданию списка community одним из следующих способов:

   - Если вы хотите создать список community в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Маршрутизация** → **Фильтры маршрутов** → **Списки community**.

   - Если вы хотите создать список community на устройстве CPE, в меню перейдите в раздел **SD-WAN** , нажмите на устройство CPE, выберите вкладку **Маршрутизация** → **Фильтры маршрутов** → **Списки community**.

   Отобразится таблица списков community.

2. Нажмите на кнопку **+ Добавить**.

3. В открывшемся окне в поле **Имя** введите имя списка community. Максимальная длина имени: 50 символов. Не используйте пробелы в этом поле.

   > Имя списка community должно быть уникальным в пределах тенанта.

4. В выпадающем списке **Тип** выберите тип списка community:

   - **Стандартный**

     Сопоставление маршрутов осуществляется на основе точного совпадения значений атрибутов community.

   - **Расширенный**

     Сопоставление маршрутов осуществляется на основе регулярных выражений.

5. Создайте правило в списке community:

   a. Нажмите на кнопку **+ Добавить**.

   b. В поле **Порядок** введите порядковый номер правила. Список community первым применяет к IPv4-префиксу правило с наименьшим значением порядкового номера. Диапазон значений: от 1 до 4 294 967 295.

   c. В раскрывающемся списке **Действие** выберите действие, которое правило выполняет с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Это значение выбрано по умолчанию.
      - **Отклонить** – запретить IPv4-префикс.

   d. Укажите критерий, по которому правило фильтрует маршруты:

      - Для стандартных списков community укажите в столбце **Community** один или несколько атрибутов community, выбрав предустановленные значения из выпадающего списка или введя вручную текстовые значения или значения в формате <число от 0 до 65535>:<число от 0 до 65535>. Вы можете комбинировать введенные вручную значения и предустановленные значения.

        Доступны следующие предустановленные значения:

        - `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`

      - Для расширенных списков community введите в поле в столбце **Регулярное выражение** регулярное выражение BGP для указания границ номеров AS. Регулярное выражение BGP является

подмножеством POSIX и использует специальный символ '_' для указания пробелов, запятых, разделителей множеств AS { }, разделителей конфедераций AS ( ), а также начала и конца строки.

Правило будет создано. Вы можете создать несколько правил и удалить правила. Для удаления правила нажмите рядом с ним на значок удаления.

6. Нажмите на кнопку **Создать**.

   Список community будет создан и отобразится в таблице.

   Вы можете использовать созданный список community в картах маршрутизации для сопоставления по префиксам или изменения атрибутов префиксов.

7. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение списка community

Вы можете изменять списки community в шаблоне CPE или на устройстве CPE. Списки community, измененные в шаблоне CPE, автоматически изменяются на всех устройствах CPE, которые используют этот шаблон CPE.

Чтобы изменить список community:

1. Перейдите к изменению списка community одним из следующих способов:

   - Если вы хотите изменить список community в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Маршрутизация** → **Фильтры маршрутов** → **Списки community**.

   - Если вы хотите изменить список community на устройстве CPE, в меню перейдите в раздел **SD-WAN**, нажмите на устройство CPE, выберите вкладку **Маршрутизация** → **Фильтры маршрутов** → **Списки community**.

   Отобразится таблица списков community.

2. Нажмите на имя списка community, который вы хотите изменить, или выберите его в таблице и нажмите на кнопку **Изменить**.

3. В открывшемся окне при необходимости измените параметры списка community. Описание параметров см. в инструкции по созданию списка community.

4. Нажмите на кнопку **Сохранить**.

   Список community будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление списка community

Вы можете удалять спиcски community в шаблоне CPE или на устройстве CPE. Списки community, удаленные в шаблоне CPE, автоматически удаляются на всех устройствах CPE, которые используют этот шаблон CPE.

Удаленные списки community невозможно восстановить.

Чтобы удалить список community:

1. Перейдите к удалению списка community одним из следующих способов:

   - Если вы хотите удалить список community в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Маршрутизация** → **Фильтры маршрутов** → **Списки community**.

   - Если вы хотите удалить список community на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Маршрутизация** → **Фильтры маршрутов** → **Списки community**.

   Отобразится таблица списков community.

2. Выберите в таблице список community, который вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Список community будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с картами маршрутизации (route maps)

Вы можете посмотреть таблицу карт маршрутизации в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы карт маршрутизации в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **Фильтры маршрутов** → **Карты маршрутизации**.

- Для просмотра таблицы карт маршрутизации на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **CPE**, нажать на устройство CPE и выбрать вкладку **Фильтры маршрутов** → **Карты маршрутизации**.

Информация о картах маршрутизации отображается в следующих столбцах таблицы:

- **Имя** – имя карты маршрутизации.
- **Унаследовано** – карта маршрутизации унаследована из шаблона CPE:
  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.
- **Порядок** – порядковый номер правила в карте маршрутизации. Карта маршрутизации первым применяет к IPv4-префиксу правило с наименьшим значением порядкового номера.
- **Действие** – действие, которое правило выполняет с IPv4-префиксом:
  - **Разрешить** – разрешить IPv4-префикс.
  - **Отклонить** – запретить IPv4-префикс.
- **Условие** – критерий, согласно которому карта маршрутизации применяет правило к IPv4-префиксу:
  - **Отсутствует** – применять правило ко всем IPv4-префиксам.
  - **Prefix-List** – применять правило к IPv4-префиксам, разрешенным указанным списком префиксов.
  - **Список community** – применять правило к IPv4-префиксам, разрешенным указанным списком community.
- **Значение** – IPv4-префикс, который должен разрешить список префиксов, чтобы карта маршрутизации применяла правило к IPv4-префиксу. В этом столбце отображается значение, только если в столбце **Условие** отображается значение **Prefix-List**.
- **Изменить атрибут** – атрибут, значение которого изменяет правило.
- **Новое значение** – значение, которое правило указывает для атрибута.
- **Управление** – действия, которые можно выполнить с картой маршрутизации.

Создание карты маршрутизации

Вы можете создать карту маршрутизации в шаблоне CPE или на устройстве CPE. Карта маршрутизации, созданная в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать карту маршрутизации:

1. Перейдите к созданию карты маршрутизации одним из следующих способов:

   - Если вы хотите создать карту маршрутизации в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации**.

   - Если вы хотите создать карту маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации** и установите флажок **Переопределить**.

   Отобразится таблица карт маршрутизации.

2. Нажмите на кнопку **+ Карта маршрутизации**.

3. В открывшемся окне в поле **Имя** введите имя карты маршрутизации. Максимальная длина имени: 50 символов. Не используйте пробелы в этом поле.

4. Создайте правило в карте маршрутизации:

   a. Нажмите на кнопку **+ Правило**.

   b. В поле **Порядок** введите порядковый номер правила. Карта маршрутизации первым применяет к IPv4-префиксу правило с наименьшим значением порядкового номера. Диапазон значений: от 1 до 4 294 967 295.

   c. В раскрывающемся списке **Действие** выберите действие, которое правило выполняет с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Это значение выбрано по умолчанию.
      - **Отклонить** – запретить IPv4-префикс.

   d. В раскрывающемся списке **Условие** выберите критерий, согласно которому карта маршрутизации применяет правило к IPv4-префиксу:

      - **Отсутствует** – применять правило ко всем IPv4-префиксам. Это значение выбрано по умолчанию.
      - **Prefix-List** – применять правило к IPv4-префиксам, разрешенным указанным списком префиксов. При выборе этого значения в раскрывающемся списке **Список префиксов** выберите созданный список префиксов.
      - **Список community** – применять правило к IPv4-префиксам, разрешенным указанным списком префиксов. При выборе этого значения в раскрывающемся списке **Список community,** выберите созданный список community.

   e. Если в раскрывающемся списке **Условие** вы выбрали **Prefix-List** или **Список community**, в раскрывающемся списке **Изменить атрибут** выберите атрибут, который правило изменяет://TODO

      - **Отсутствует** – не изменять значения атрибутов. Это значение выбрано по умолчанию.
      - **IP next-hop** – изменять значение атрибута next hop на указанный IPv4-адрес. При выборе этого значения в поле **Новое значение** введите IPv4-адрес.
      - **Local preference** – изменять значение атрибута local preference на указанное значение. При выборе этого значения в поле **Новое значение** введите значение атрибута local preference. Диапазон значений: от 0 до 4 294 967 295.
      - **Metric** – изменять значение атрибута MED на указанное значение. При выборе этого значения в поле **Новое значение** введите значение атрибута MED. Диапазон значений: от 0 до 4 294 967 295.
      - **AS path preprend** – добавлять номер автономной системы в атрибут as path. При выборе этого значения в поле **Новое значение** введите номер автономной системы. Вы можете ввести несколько номеров через пробел. Диапазон значений: от 0 до 4 294 967 295.

Правило будет создано. Вы можете создать несколько правил и удалить правила. Для удаления правила нажмите рядом с ним на значок удаления ✕.

5. Нажмите на кнопку **Создать**.

   Карта маршрутизации будет создана и отобразится в таблице.

6. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение карты маршрутизации

Вы можете изменить карту маршрутизации в шаблоне CPE или на устройстве CPE. Карта маршрутизации, измененная в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

> Если вы хотите, чтобы изменения, внесенные вами в карту маршрутизации, были мгновенно применены к BGP-соседям или группам BGP-соседей, которые используют карту маршрутизации, вам нужно установить флажок **BFD** или **Soft-reconfiguration inbound** при создании или изменении BGP-соседа, или группы BGP-соседей.

Чтобы изменить карту маршрутизации:

1. Перейдите к изменению карты маршрутизации одним из следующих способов:

   - Если вы хотите изменить карту маршрутизации в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и в отобразившейся области настройки выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации**.

   - Если вы хотите изменить карту маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, в отобразившейся области настройки выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации** и установите флажок **Переопределить**.

   Отобразится таблица карт маршрутизации.

2. Нажмите на кнопку **Изменить** рядом с картой маршрутизации, которую вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры карты маршрутизации. Описание параметров см. в инструкции по созданию карты маршрутизации.

4. Нажмите на кнопку **Сохранить**.

   Карта маршрутизации будет изменена и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление карты маршрутизации

Вы можете удалить карту маршрутизации в шаблоне CPE или на устройстве CPE. Карта маршрутизации, удаленная в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE.

Удаленные карты маршрутизации невозможно восстановить.

Чтобы удалить карту маршрутизации:

1. Перейдите к удалению карты маршрутизации одним из следующих способов:

   - Если вы хотите удалить карту маршрутизации в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации**.

   - Если вы хотите удалить карту маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации** и установите флажок **Переопределить**.

   Отобразится таблица карт маршрутизации.

2. Нажмите на кнопку **Удалить** рядом с картой маршрутизации, которую вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Карта маршрутизации будет удалена и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Маршрутизация на основе политик (PBR)

Помимо маршрутизации на основе стандартных свойств пакетов, таких как IP-адрес назначения, Kaspersky SD-WAN поддерживает маршрутизацию на основе политик (Policy-based Routing, PBR). Этот тип маршрутизации основан на использовании политик – наборах правил маршрутизации, или IP-правил, создаваемых пользователем (администратором или тенантом) и сохраняемых на устройстве. Ниже приведены примеры пользовательских сценариев использования PBR-маршрутизации:

- Перенаправление трафика для сетей, определенных пользователем, в обход межсетевого экрана в случае проблем с межсетевым экраном.

- Перенаправление трафика для сетей, определенных пользователем, в интернет через SD-WAN в сторону шлюза, который является единой точкой выхода в интернет для всех CPE.

Вы можете создавать и просматривать правила маршрутизации как в командной строке на устройстве CPE с помощью команд пакета утилит iproute2, так и в графическом интерфейсе оркестратора. В этом разделе дается описание работы с правилами маршрутизации в графическом интерфейсе оркестратора.

Работа с IP-правилами маршрутизации

Вы можете посмотреть таблицу IP-правил в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы IP-правил в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон CPE и выбрать в боковой панели раздел **PBR**.
- Для просмотра таблицы IP-правил на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **CPE**, нажать на устройство CPE и выбрать в боковой панели раздел **PBR**.

Информация о IP-правилах отображается в следующих столбцах таблицы:

- **Приоритет** – приоритет правила. Чем ниже значение, тем раньше применяется правило.
- **Статус** – статус правила. Возможные значения:
  - **Включено** – правило активно;
  - **Выключено** – правило неактивно.
- **IP-протокол** – IP-протокол. Возможны следующие значения:
  - TCP
  - UDP
  - ICMP
  - SCTP
  - AH
  - ESP
  - GRE
  - IPIP
- **Сетевой интерфейс источника** – входящий интерфейс для сопоставления. Если интерфейс является петлевым, то правило соответствует только пакетам, исходящим из этого хоста.
- **Исходящий порт** – порт источника.
- **Исходящий префикс сети** – хост или сеть источника.
- **Выходной сетевой интерфейс** – исходящий интерфейс для сопоставления. Исходящий интерфейс доступен только для пакетов, исходящих из локальных сокетов, привязанных к устройству.
- **Конечный порт** – порт назначения.
- **Конечный префикс сети** – хост или сеть назначения.

- **VRF** – VRF, в котором выполняется поиск маршрутов.
- **Действия** – действия, которые можно выполнить с IP-правилом (включить, выключить, изменить, удалить).

Создание IP-правила

Вы можете создать IP-правило в шаблоне CPE или на устройстве CPE. IP-правила, созданные в шаблоне CPE, будут автоматически созданы на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать IP-правило:

1. Перейдите к созданию IP-правила одним из следующих способов:
   - Если вы хотите создать IP-правило в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите в боковой панели раздел **PBR**.
   - Если вы хотите создать IP-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите в боковой панели раздел **PBR**.

   Отобразится таблица с IP-правилами.
2. Нажмите на кнопку **+ IP-правило**.
3. В открывшемся окне в поле **Приоритет** введите приоритет правила. Чем ниже значение, тем раньше применяется правило. Значение должно быть уникальным.
4. В раскрывающемся списке **IP-протокол** выберите IP-протокол. Возможны следующие значения:
   - TCP
   - UDP
   - ICMP
   - SCTP
   - AH
   - ESP
   - GRE
   - IPIP

5. Укажите необходимые параметры источника и назначения для IP-правила в блоках **Источник** и **Назначение**:

   - Укажите тип источника или назначения, выбрав нужный вариант параметра **Тип**: хост или сеть.
   - В зависимости от выбранного в поле **Тип** варианта укажите в поле ниже:
     - IP-адрес источника или назначения, если вы выбрали тип **Хост** (поле при этом имеет название **IP-адрес**;
     - IP-адрес и маску источника или назначения, если вы выбрали тип **Сеть** (поле при этом имеет название **IP/маска**.
   - В поле **Порт** укажите порт источника или назначения.

     Допускается ввод как одного значения, так и диапазона значений от 1 до 65 535 через дефис, например: `443`, `1024-65535`.
   - В раскрывающемся списке **Псевдоним сетевого интерфейса** выберите интерфейс источника (входящий интерфейс) или назначения (исходящий интерфейс).

     Если входящий интерфейс является петлевым, то правило будет соответствовать только пакетам, исходящим из этого хоста. Исходящий интерфейс доступен только для пакетов, исходящих из локальных сокетов, привязанных к устройству.

6. В раскрывающемся списке **Искать в VRF** выберите VRF, в котором должен выполняться поиск маршрутов.

   Если вы выбрали main/254, то в блоке **Назначение** вам необходимо указать IP-адрес источника, отличный от 0.0.0.0/0, иначе правило невозможно будет сохранить.

7. Нажмите на кнопку **Создать**.

   IP-правило будет создано и отобразится в таблице.

8. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE.

Изменение IP-правила

Вы можете изменить IP-правила в шаблоне CPE или на устройстве CPE. IP-правила, измененные в шаблоне CPE, автоматически изменяются на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить IP-правило:

1. Перейдите к изменению IP-правила одним из следующих способов:

   - Если вы хотите изменить IP-правило в шаблоне CPE:

     - Перейдите в меню в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите в боковой панели раздел **PBR**.

     - В отобразившейся таблице IP-правил в столбце **Действия** нажмите на кнопку **Изменить** для правила, которое вы хотите изменить.

   - Если вы хотите изменить IP-правило на устройстве CPE:

     - Перейдите в меню в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE и выберите в боковой панели раздел **PBR**.

     - В отобразившейся таблице IP-правил в столбце **Действия** нажмите на кнопку **Изменить** для правила, которое вы хотите изменить. Если IP-правило было унаследовано из шаблона, предварительно установите для него флажок **Переопределить**, чтобы отобразилась кнопка **Изменить**.

2. В открывшемся окне измените требуемые параметры IP-правила. Описание параметров можно найти в инструкции по созданию IP-правила.

3. Нажмите на кнопку **Сохранить**.

   IP-правило будет изменено и обновится в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление IP-правила

Вы можете удалить IP-правила в шаблоне CPE или на устройстве CPE. IP-правила, удаленные в шаблоне CPE, автоматически удаляются на всех устройствах CPE, которые используют шаблон CPE. Вы можете удалить на устройстве CPE только те IP-правила, которые были добавлены непосредственно на устройстве, и не сможете удалить IP-правила, унаследованные из шаблона.

Удаленные IP-правила невозможно восстановить.

Чтобы удалить IP-правило:

1. Перейдите к удалению IP-правила одним из следующих способов:

   - Если вы хотите удалить IP-правило в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите в боковой панели раздел **PBR**.

   - Если вы хотите удалить не унаследованное из шаблоне CPE IP-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите в боковой панели раздел **PBR**.

   Отобразится таблица IP-правил.

2. Нажмите на кнопку **Удалить** рядом с IP-правилом, которое вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   IP-правило будет удалено и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

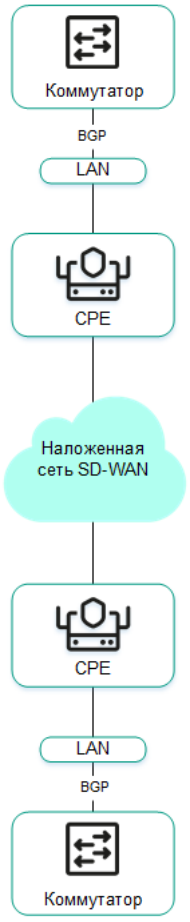
Обмен маршрутами по протоколу BGP

Kaspersky SD-WAN поддерживает протокол динамической маршрутизации BGP (Border Gateway Protocol) для обмена маршрутной информацией между устройствами CPE и внешними сетевыми устройствами. Вы можете устанавливать внутренние сессии iBGP (internal BGP) и внешние сессии eBGP (external BGP).

Поддерживается создание отдельных BGP-соседей (англ. BGP peers) и групп BGP-соседей (англ. BGP peer groups). С группами BGP-соседей устанавливаются динамические TCP-сессии.

На рисунках ниже представлены примеры использования протокола динамической маршрутизации BGP в решении:

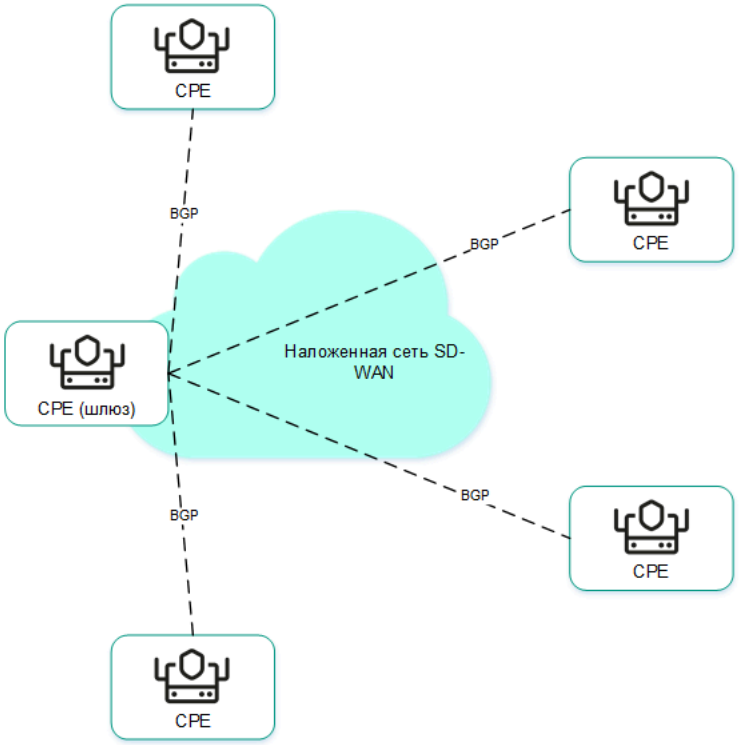
- Подключение нескольких клиентских площадок к сети L3 SD-WAN по BGP.



- Подключение устройств CPE к операторской сети IP/MPLS по BGP.



- Использование BGP для настройки связности устройств CPE внутри домена.



Настройка основных параметров BGP

Вы можете настроить основные параметры BGP в шаблоне CPE или на устройстве CPE. Параметры BGP, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

Чтобы настроить основные параметры BGP:

1. Перейдите к настройке основных параметров BGP одним из следующих способов:

   - Если вы хотите настроить основные параметры BGP в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и в открывшемся окне выберите в боковой панели раздел **BGP**.

   - Если вы хотите настроить основные параметры BGP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, в открывшемся окне выберите в боковой панели раздел **BGP** и установите флажок **Переопределить**, в результате чего разблокируется поле **Автономная система.**

2. В поле **Автономная система** укажите номер автономной системы (число: от 1 до 4 294 967 295). Указанная автономная система будет использована для всех экземпляров BGP, создаваемых на этом устройстве или в этом шаблоне CPE, и будет отображаться в поле **AS**.

   После того, как вы указали номер автономной системы, станет доступна кнопка **+ BGP**.

3. В списке **Экземпляр BGP по умолчанию** выберите экземпляр BGP, который должен использоваться по умолчанию. Если ни один экземпляр BGP еще не создан, создайте его, используя шаги ниже, затем выберите созданный экземпляр.

4. Создайте один или несколько экземпляров BGP. Для этого:

    1. Нажмите на кнопку кнопку **+ BGP**. Появится рабочая область добавления экземпляра BGP.

    2. По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры BGP.

    3. В раскрывающемся списке **BGP** выберите **Включено**. Значение по умолчанию: **Выключено**.

    4. В раскрывающемся списке **VRF** выберите существующий VRF, в который необходимо передавать BGP-маршруты. В списке показаны только те VRF, которые не ассоциированы с другими экземплярами BGP на устройстве или в шаблоне CPE.

    5. В поле **Router ID** введите IPv4-адрес, который вы хотите назначить идентификатору маршрутизатора (англ. router ID) устройства CPE. Если вы хотите назначить IPv4-адрес из указанного диапазона IP-адресов, выполните следующие действия:

    6. Установите флажок **Router ID из диапазона IP**. Этот флажок снят по умолчанию.

    7. В раскрывающемся списке **Диапазон IP** выберите созданный диапазон IP-адресов.

    8. При необходимости в поле **Лимит маршрутов** введите максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 8.

    9. При необходимости установите следующие флажки:

    10. Установите флажок **Всегда сравнивать MED**, чтобы устройство CPE сравнивало атрибут MED (multi-exit discriminator) маршрутов, анонсированных из разных автономных систем.

        Вам нужно убедиться, что флажок установлен для всех устройств CPE в вашей автономной системе. В противном случае при обмене маршрутной информацией могут возникать петли маршрутизации.

        - Установите флажок **Graceful restart (режим helper)**, чтобы включить перезагрузку Graceful restart на устройстве CPE.

          По умолчанию флажки сняты.

    11. Если вы хотите, чтобы устройство CPE по умолчанию не обменивалось IPv4-маршрутами с BGP-соседями, снимите флажок **IPv4 unicast-маршруты по умолчанию**. Этот флажок установлен по умолчанию.

    12. Если вы хотите настроить BGP-таймеры, выполните следующие действия:

    13. Установите флажок **BGP-таймеры**. Этот флажок снят по умолчанию.

        a. В поле **Keepalive (сек.)** введите интервал времени в секундах для отправки устройством CPE контрольных пакетов BGP-соседям. Диапазон значений: от 0 до 65 535.

        b. В поле **Holdtime (сек.)** введите интервал времени в секундах для получения устройством CPE контрольных пакетов от BGP-соседей. Если в течение указанного времени от BGP-соседа не поступает контрольных пакетов, устройство CPE считает его недоступным. Диапазон значений: от 0 до 65 535.

14. Если вы хотите настроить перераспределение маршрутов в BGP, в блоке **Перераспределение маршрутов** выполните следующие действия:

    a. Установите флажки рядом с типами маршрутов:

    - **Kernel** – перераспределять Kernel-маршруты, генерируемые операционной системой устройства CPE.
    - **Connected** – перераспределять маршруты, напрямую подключенные к сетевым интерфейсам устройства CPE.
    - **Статический** – перераспределять статические маршруты.
    - **OSPF** – перераспределять OSPF-маршруты.

    По умолчанию флажки сняты.

    b. В раскрывающемся списке **Карта маршрутизации** выберите созданную карту маршрутизации для перераспределяемых маршрутов.

    c. В поле **Метрика** введите метрику перераспределяемых маршрутов. Диапазон значений: от 0 до 16 777 214.

15. Если вы хотите, чтобы устройство CPE анонсировало BGP-соседям указанную подсеть, выполните следующие действия:

    a. В блоке **Сети** нажмите на кнопку **+ Сеть**.

    b. В поле **Сеть** введите IPv4-префикс подсети.

    c. В раскрывающемся списке **Карта маршрутизации** выберите созданную карту маршрутизации для подсети.

    Подсеть будет указана и отобразится в блоке **Сети**. Вы можете указать несколько подсетей и удалить подсети. Для удаления подсети нажмите рядом с ней на значок удаления ✕.

16. При необходимости также настройте соответствующие параметры экземпляра BGP на вкладках **BGP-соседи**, **Группы BGP-соседей** и **Обмен маршрутами**.

17. В нижней части рабочей области добавления экземпляра BGP нажмите на кнопку **Сохранить**, чтобы сохранить параметры экземпляра BGP.

    Экземпляр BGP будет сохранен и появится в таблице экземпляров BGP в области настройки.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с BGP-соседями (BGP peers)

Чтобы просмотреть или изменить таблицу BGP-соседей экземпляра BGP в шаблоне CPE или на устройстве CPE:

1. Перейдите в раздел **BGP**. Для этого:

   - Чтобы просмотреть или изменить таблицу BGP-соседей в шаблоне CPE, перейдите в меню в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите в боковой панели области настройки **BGP**.

   - Чтобы просмотреть или изменить таблицу BGP-соседей на устройстве CPE, перейдите в меню в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE и выберите в боковой панели области настройки **BGP**.

2. Откройте существующий экземпляр BGP, нажав в таблице на **Изменить** в нужной строке, либо создайте новый экземпляр BGP.

3. В области настройки параметров экземпляра BGP откройте вкладку **BGP-соседи**.

Информация о BGP-соседях отображается в следующих столбцах таблицы:

- **IP соседа** – IPv4-адрес BGP-соседа.
- **Имя** – имя BGP-соседа.
- **Описание** – краткое описание BGP-соседа.
- **Унаследовано** – BGP-сосед унаследован из шаблона CPE:
  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.
- **Удаленная AS** – номер автономной системы BGP-соседа.
- **Выключить** – BGP-сосед выключен и с ним не установлена TCP-сессия:
  - **Да**.
  - **Нет**.
- **Вес** – вес маршрутов, анонсируемых BGP-соседом.
- **Управление** – действия, которые можно выполнить с BGP-соседом.

Создание BGP-соседа

Вы можете создать BGP-соседа в шаблоне CPE или на устройстве CPE. BGP-сосед, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE. Максимальное количество динамических BGP-соседей: 512.

Чтобы создать BGP-соседа:

1. Перейдите к созданию BGP-соседа одним из следующих способов:

   - Если вы хотите создать BGP-соседа в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BGP → BGP-соседи**.

   - Если вы хотите создать BGP-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **BGP → BGP-соседи** и установите флажок **Переопределить**.

   Отобразится таблица BGP-соседей.

2. Нажмите на кнопку **+ BGP-сосед**.

3. В открывшемся окне в поле **Имя** введите имя BGP-соседа. Максимальная длина имени: 50 символов.

4. Если вы хотите выключить BGP-соседа и не устанавливать с ним TCP-сессию, установите флажок **Выключить BGP-соседа**. Этот флажок снят по умолчанию.

5. В поле **IP соседа** введите IPv4-адрес BGP-соседа.

6. В поле **Удаленная AS** введите номер автономной системы BGP-соседа. Диапазон значений: от 1 до 4 294 967 295.

7. При необходимости в поле **Описание** введите краткое описание BGP-соседа.

8. Если вы хотите, чтобы устройство CPE использовало пароль при установке TCP-сессии с BGP-соседом, в поле **Пароль** введите пароль. Для успешной установки TCP-сессии между двумя BGP-соседями они должны использовать одинаковый пароль. Вы можете просмотреть введенный пароль, нажав на значок просмотра 👁.

9. При необходимости в поле **IP-адрес для установления BGP-сессии** введите IPv4-адрес loopback-интерфейса, который устройство CPE передает BGP-соседу при установке TCP-сессии.

10. Если TCP-сессия между устройством CPE и BGP-соседом устанавливается не напрямую, в поле **Хопы для eBGP** введите количество хопов (англ. hops) между устройством CPE и BGP-соседом. Диапазон значений: от 1 до 255.

11. Если вы хотите настроить BGP-таймеры, выполните следующие действия:

    a. Установите флажок **Уникальные BGP-таймеры**. Этот флажок снят по умолчанию.

    b. В поле **Keepalive (сек.)** введите интервал времени в секундах для отправки устройством CPE контрольных пакетов BGP-соседу. Диапазон значений: от 0 до 65 535.

    c. В поле **Holdtime (сек.)** введите интервал времени в секундах для получения устройством CPE контрольных пакетов от BGP-соседа. Если в течение указанного времени от BGP-соседа не поступает контрольных пакетов, устройство CPE считает BGP-соседа недоступным. Диапазон значений: от 0 до 65 535.

12. Если вы хотите использовать протокол BFD для обнаружения потери связности, установите флажок **BFD**. Этот флажок снят по умолчанию. Когда флажок установлен, изменения, внесенные вами в карту маршрутизации, мгновенно применяются к BGP-соседу, если BGP-сосед использует карту маршрутизации. Вы можете выбрать карту маршрутизации для BGP-соседа на шаге 14 этой инструкции.

13. Если вы хотите указать дополнительные параметры BGP-соседа, выполните следующие действия:

    a. Выберите вкладку **Расширенные параметры**.

    Отобразятся дополнительные параметры BGP-соседа.

    b. При необходимости установите следующие флажки:

    - Установите флажок **Soft-reconfiguration inbound**, чтобы хранить анонсированные BGP-соседом маршруты локально на устройстве CPE. Использование этой функции снижает количество памяти, доступной на устройстве CPE. Когда флажок установлен, изменения, внесенные вами в карту маршрутизации, мгновенно применяются к BGP-соседу, если BGP-сосед использует карту маршрутизации. Вы можете выбрать карту маршрутизации для BGP-соседа на шаге 14 этой инструкции.

    - Установите флажок **Неизменный атрибут AS path**, чтобы не изменять атрибут AS path маршрутов, которые устройство CPE анонсирует BGP-соседу.

    - Установите флажок **Разрешить AS in**, чтобы BGP-соседи могли анонсировать устройству CPE маршруты с атрибутом AS path, значением которого является номер автономной системы устройства CPE.

    - Установите флажок **Неизменный атрибут next-hop**, чтобы не изменять атрибут next hop маршрутов, которые устройство CPE анонсирует BGP-соседу.

    - Установите флажок **Собственный IP как next-hop**, чтобы использовать IPv4-адрес устройства CPE как значение атрибута next-hop при анонсировании маршрутов BGP-соседу.

    - Установите флажок **Неизменный атрибут MED**, чтобы не изменять атрибут MED маршрутов, которые устройство CPE анонсирует BGP-соседу.

    - Установите флажок **Клиент route reflector**, чтобы назначить устройству CPE роль *Route Reflector*, а BGP-соседу – *клиент Route Reflector*. Вы можете установить флажок только для BGP-соседа, который находится в той же автономной системе, что устройство CPE.

    По умолчанию флажки сняты.

    c. В поле **Локальная AS** введите номер дополнительной автономной системы, который устройство CPE передает BGP-соседу. Диапазон значений: от 1 до 4 294 967 295.

    d. В поле **Вес** введите вес маршрутов, анонсируемых BGP-соседом. Чем больше вес маршрута, тем больше его приоритет. Диапазон значений: от 0 до 65 535.

    e. В поле **Лимит префиксов** введите максимальное количество маршрутов, которое BGP-сосед может анонсировать устройству CPE. Диапазон значений: от 1 до 4 294 967 295.

    f. Если вы хотите, чтобы устройство CPE анонсировало BGP-соседу маршруты с атрибутом community, установите флажок **Отправлять community** и в раскрывающемся списке выберите тип атрибута:

    - **Все** – все доступные типы атрибута community.

    - **Standard и extended community**.

    - **Extended community**.

    - **Large community**.

- **Standard community**.

Этот флажок снят по умолчанию.

a. Если вы хотите, чтобы устройство CPE анонсировало BGP-соседу маршрут по умолчанию 0.0.0.0/0, установите флажок **Маршрут по умолчанию**. Этот флажок снят по умолчанию. Вы можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать созданную карту маршрутизации для маршрута по умолчанию 0.0.0.0/0.

14. Если вы хотите настроить фильтрацию маршрутов для BGP-соседа, выполните следующие действия:

a. Выберите вкладку **Фильтрация**.

Отобразятся параметры фильтрации маршрутов.

b. В блоке **Карта маршрутизации** выберите созданные карты маршрутизации:

1. В раскрывающемся списке **Входящие** выберите карту маршрутизации для маршрутов, которые BGP-сосед анонсирует устройству CPE.

2. В раскрывающемся списке **Исходящие** выберите карту маршрутизации для маршрутов, которые устройство CPE анонсирует BGP-соседу.

c. В блоке **Список префиксов** выберите созданные списки префиксов:

1. В раскрывающемся списке **Входящие** выберите список префиксов для маршрутов, которые BGP-сосед анонсирует устройству CPE.

2. В раскрывающемся списке **Исходящие** выберите список префиксов для маршрутов, которые устройство CPE анонсирует BGP-соседу.

d. В блоке **Список управления доступом** выберите созданные списки управления доступом:

1. В раскрывающемся списке **Входящие** выберите список управления доступом для маршрутов, которые BGP-сосед анонсирует устройству CPE.

2. В раскрывающемся списке **Исходящие** выберите список управления доступом для маршрутов, которые устройство CPE анонсирует BGP-соседу.

15. Нажмите на кнопку **Создать**.

BGP-сосед будет создан и отобразится в таблице.

16. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение BGP-соседа

Вы можете изменить BGP-соседа в шаблоне CPE или на устройстве CPE. BGP-сосед, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете изменить на устройстве CPE BGP-соседа, унаследованного из шаблона CPE.

Чтобы изменить BGP-соседа:

1. Перейдите к изменению BGP-соседа одним из следующих способов:

   - Если вы хотите изменить BGP-соседа в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BGP** → **BGP-соседи**.

   - Если вы хотите изменить BGP-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **BGP** → **BGP-соседи** и установите флажок **Переопределить**.

   Отобразится таблица BGP-соседей.

2. Нажмите на кнопку **Изменить** рядом с BGP-соседом, которого вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры BGP-соседа. Описание параметров см. в инструкции по созданию BGP-соседа.

4. Нажмите на кнопку **Сохранить**.

   BGP-сосед будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление BGP-соседа

Вы можете удалить BGP-соседа в шаблоне CPE или на устройстве CPE. BGP-сосед, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете удалить на устройстве CPE BGP-соседа, унаследованного из шаблона CPE.

Удаленных BGP-соседей невозможно восстановить.

Чтобы удалить BGP-соседа:

1. Перейдите к удалению BGP-соседа одним из следующих способов:

   - Если вы хотите удалить BGP-соседа в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BGP** → **BGP-соседи**.

   - Если вы хотите удалить BGP-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **BGP** → **BGP-соседи** и установите флажок **Переопределить**.

   Отобразится таблица BGP-соседей.

2. Нажмите на кнопку **Удалить** рядом с BGP-соседом, которого вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   BGP-сосед будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с группами BGP-соседей (BGP peer groups)

Чтобы просмотреть или изменить таблицу групп BGP-соседей экземпляра BGP в шаблоне CPE или на устройстве CPE:

1. Перейдите в раздел **BGP**. Для этого:

   - Чтобы просмотреть или изменить таблицу групп BGP-соседей в шаблоне CPE, перейдите в меню в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите в боковой панели области настройки **BGP**.

   - Чтобы просмотреть или изменить таблицу групп BGP-соседей на устройстве CPE, перейдите в меню в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите в боковой панели области настройки **BGP**.

2. Откройте существующий экземпляр BGP, нажав в таблице на **Изменить** в нужной строке, либо создайте новый экземпляр BGP.

3. В области настройки параметров экземпляра BGP откройте вкладку **Группы BGP-соседей**.

Информация о группах BGP-соседей отображается в следующих столбцах таблицы:

- **Имя** – имя группы BGP-соседей.
- **Диапазон BGP** – IPv4-префикс группы BGP-соседей.
- **Описание** – краткое описание группы BGP-соседей.
- **Унаследовано** – группа BGP-соседей унаследована из шаблона CPE.

  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.

- **Удаленная AS** – номер автономной системы группы BGP-соседей.
- **Выключить** – группа BGP-соседей выключена и с ней не установлена TCP-сессия:

  - **Да**.
  - **Нет**.

- **Вес** – вес маршрутов, анонсируемых группой BGP-соседей.
- **Управление** – действия, которые можно выполнить с группой BGP-соседей.

Создание группы BGP-соседей

Вы можете создать группу BGP-соседей в шаблоне CPE или на устройстве CPE. Группа BGP-соседей, созданная в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать группу BGP-соседей:

1. Перейдите к созданию группы BGP-соседей одним из следующих способов:
   - Если вы хотите создать группу BGP-соседей в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BGP** → **Группы BGP-соседей**.
   - Если вы хотите создать группу BGP-соседей на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **BGP** → **Группы BGP-соседей** и установите флажок **Переопределить**.

   Отобразится таблица групп BGP-соседей.
2. Нажмите на кнопку **+ Группа BGP-соседей**.
3. В открывшемся окне в поле **Имя** введите имя группы BGP-соседей. Максимальная длина имени: 50 символов.
4. Если вы хотите выключить группу BGP-соседей и не устанавливать с ней TCP-сессию, установите флажок **Выключить группу BGP-соседей**. Этот флажок снят по умолчанию.
5. В поле **Диапазон BGP** введите IPv4-префикс группы BGP-соседей.
6. В поле **Удаленная AS** введите номер автономной системы группы BGP-соседей. Диапазон значений: от 1 до 4 294 967 295.
7. При необходимости в поле **Описание** введите краткое описание группы BGP-соседей.
8. Если вы хотите, чтобы устройство CPE использовало пароль при установке TCP-сессии с группой BGP-соседей, в поле **Пароль** введите пароль. Для успешной установки TCP-сессии между двумя BGP-соседями они должны использовать одинаковый пароль. Вы можете просмотреть введенный пароль, нажав на значок просмотра 👁.
9. В поле **IP-адрес для установления BGP-сессии** введите IPv4-адрес loopback-интерфейса, который устройство CPE передает группе BGP-соседей при установке TCP-сессии.
10. Если TCP-сессия между устройством CPE и группой BGP-соседей устанавливается не напрямую, в поле **Хопы для eBGP** введите количество хопов (англ. hops) между устройством CPE и группой BGP-соседей. Диапазон значений: от 1 до 255.

11. Если вы хотите настроить BGP-таймеры, выполните следующие действия:

    a. Установите флажок **Уникальные BGP-таймеры**. Этот флажок снят по умолчанию.

    b. В поле **Keepalive (сек.)** введите интервал времени в секундах для отправки устройством CPE контрольных пакетов группе BGP-соседей. Диапазон значений: от 0 до 65 535.

    c. В поле **Holdtime (сек.)** введите интервал времени в секундах для получения устройством CPE контрольных пакетов от группы BGP-соседей. Если в течение указанного времени от BGP-соседа не поступает контрольных пакетов, устройство CPE считает BGP-соседа недоступным. Диапазон значений: от 0 до 65 535.

12. Если вы хотите использовать протокол BFD для обнаружения потери связности, установите флажок **BFD**. Этот флажок снят по умолчанию. Когда флажок установлен, изменения, внесенные вами в карту маршрутизации, мгновенно применяются к группе BGP-соседей, если группа BGP-соседей использует карту маршрутизации. Вы можете выбрать карту маршрутизации для группы BGP-соседей на шаге 14 этой инструкции.

13. Если вы хотите указать дополнительные параметры группы BGP-соседей, выполните следующие действия:

    a. Выберите вкладку **Расширенные параметры**.

    Отобразятся дополнительные параметры группы BGP-соседей.

    b. При необходимости установите следующие флажки:

    - Установите флажок **Soft-reconfiguration inbound**, чтобы хранить анонсированные группой BGP-соседей маршруты локально на устройстве CPE. Использование этой функции снижает количество памяти, доступной на устройстве CPE. Когда флажок установлен, изменения, внесенные вами в карту маршрутизации, мгновенно применяются к группе BGP-соседей, если группа BGP-соседей использует карту маршрутизации. Вы можете выбрать карту маршрутизации для группы BGP-соседей на шаге 14 этой инструкции.

    - Установите флажок **Неизменный атрибут AS path**, чтобы не изменять атрибут AS path маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

    - Установите флажок **Разрешить AS in**, чтобы группа BGP-соседей могла анонсировать устройству CPE маршруты с атрибутом AS path, значением которого является номер автономной системы устройства CPE.

    - Установите флажок **Неизменный атрибут next-hop**, чтобы не изменять атрибут next hop маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

    - Установите флажок **Собственный IP как next-hop**, чтобы использовать IPv4-адрес устройства CPE как значение атрибута next-hop при анонсировании маршрутов группе BGP-соседей.

    - Установите флажок **Неизменный атрибут MED**, чтобы не изменять атрибут MED маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

    - Установите флажок **Клиент route reflector**, чтобы назначить устройству CPE роль *Route Reflector*, а группе BGP-соседей – *клиент Route Reflector*. Вы можете установить флажок только для группы BGP-соседей, которая находится в той же автономной системе, что устройство CPE.

    По умолчанию флажки сняты.

    c. В поле **Локальная AS** введите номер дополнительной автономной системы, который устройство CPE передает группе BGP-соседей. Диапазон значений: от 1 до 4 294 967 295.

    d. В поле **Вес** введите вес маршрутов, анонсируемых группой BGP-соседей. Чем больше вес маршрута, тем больше его приоритет. Диапазон значений: от 0 до 65 535.

    e. В поле **Лимит префиксов** введите максимальное количество маршрутов, которое группа BGP-соседей может анонсировать устройству CPE. Диапазон значений: от 1 до 4 294 967 295.

    f. Если вы хотите, чтобы устройство CPE анонсировало группе BGP-соседей маршруты с атрибутом community, установите флажок **Отправлять community** и в раскрывающемся списке выберите тип отправляемого атрибута:

    - **Все** – все доступные типы атрибута community.

    - **Standard и extended community**.

    - **Extended community**.

- **Large community**.
- **Standard community**.

Этот флажок снят по умолчанию.

a. Если вы хотите, чтобы устройство CPE анонсировало группе BGP-соседей маршрут по умолчанию 0.0.0.0/0, установите флажок **Маршрут по умолчанию**. Этот флажок снят по умолчанию. Вы можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать созданную карту маршрутизации для маршрута по умолчанию 0.0.0.0/0.

14. Если вы хотите настроить фильтрацию маршрутов для группы BGP-соседей, выполните следующие действия:

a. Выберите вкладку **Фильтрация**.

Отобразятся параметры фильтрации маршрутов.

b. В блоке **Карта маршрутизации** выберите созданные карты маршрутизации:

1. В раскрывающемся списке **Входящие** выберите карту маршрутизации для маршрутов, которые группа BGP-соседей анонсирует устройству CPE.
2. В раскрывающемся списке **Исходящие** выберите карту маршрутизации для маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

c. В блоке **Список префиксов** выберите созданные списки префиксов:

1. В раскрывающемся списке **Входящие** выберите список префиксов, которые группа BGP-соседей анонсирует устройству CPE.
2. В раскрывающемся списке **Исходящие** выберите список префиксов для маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

d. В блоке **Список управления доступом** выберите созданные списки управления доступом:

1. В раскрывающемся списке **Входящие** выберите список управления доступом для маршрутов, которые группа BGP-соседей анонсирует устройству CPE.
2. В раскрывающемся списке **Исходящие** выберите список управления доступом для маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

15. Нажмите на кнопку **Создать**.

Группа BGP-соседей будет создана и отобразится в таблице.

16. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение группы BGP-соседей

Вы можете изменить группу BGP-соседей в шаблоне CPE или на устройстве CPE. Группа BGP-соседей, измененная в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете изменить на устройстве CPE группу BGP-соседей, унаследованную из шаблона CPE.

Чтобы изменить группу BGP-соседей:

1. Перейдите к изменению группы BGP-соседей одним из следующих способов:

   - Если вы хотите изменить группу BGP-соседей в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BGP** → **Группы BGP-соседей**.

   - Если вы хотите изменить группу BGP-соседей на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **BGP** → **Группы BGP-соседей** и установите флажок **Переопределить**.

   Отобразится таблица групп BGP-соседей.

2. Нажмите на кнопку **Изменить** рядом с группой BGP-соседей, которую вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры группы BGP-соседей. Описание параметров см. в инструкции по созданию группы BGP-соседей.

4. Нажмите на кнопку **Сохранить**.

   Группа BGP-соседей будет изменена и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление группы BGP-соседей

Вы можете удалить группу BGP-соседей в шаблоне CPE или на устройстве CPE. Группа BGP-соседей, удаленная в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете удалить на устройстве CPE группу BGP-соседей, унаследованную из шаблона CPE.

Удаленные группы BGP-соседей невозможно восстановить.

Чтобы удалить группу BGP-соседей:

1. Перейдите к удалению группы BGP-соседей одним из следующих способов:

   - Если вы хотите удалить группу BGP-соседей в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BGP** → **Группы BGP-соседей**.

   - Если вы хотите удалить группу BGP-соседей на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **BGP** → **Группы BGP-соседей** и установите флажок **Переопределить**.

   Отобразится таблица групп BGP-соседей.

2. Нажмите на кнопку **Удалить** рядом с группой BGP-соседей, которую вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Группа BGP-соседей будет удалена и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Настройка параметров обмена маршрутами между VRF (Inter-VFR Route Leaking)

Чтобы просмотреть или изменить параметры обмена маршрутами между VRF для экземпляра BGP в шаблоне CPE или на устройстве CPE:

1. Перейдите в раздел **BGP**. Для этого:

   - Чтобы просмотреть или изменить параметры обмена маршрутами между VRF в шаблоне CPE, перейдите в меню в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите в боковой панели области настройки **BGP**.

   - Чтобы просмотреть или изменить обмена маршрутами между VRF на устройстве CPE, перейдите в меню в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE и выберите в боковой панели области настройки **BGP**.

2. Откройте существующий экземпляр BGP, нажав в таблице на **Изменить** в нужной строке, либо создайте новый экземпляр BGP.

3. В области настройки параметров экземпляра BGP откройте вкладку **Обмен маршрутами**.

4. При необходимости настройте следующие параметры обмена маршрутами между VRF:

   - В поле **Route Distinguisher** укажите атрибут Route Distinguisher (RD) для обмена марштурами (уникальный идентификатор для различения маршрутов). Возможна запись в одном из двух форматов:

     - Номер автономной системы (число от 0 до 4294967295) : идентификатор (число от 0 до 65535). Пример: `100:65000`.

     - IPv4-адрес : идентификатор (число от 0 до 65535). Пример: `1.2.3.4:15`.

     Вы можете автоматически сгенерировать атрибут Route Distinguisher, установив флажок **Автоматически сгенерировать** (по умолчанию установлен).

   - В блоке **Route Target для экспорта** добавьте с помощью кнопки **Добавить** одно или несколько значений Route Target (RT) для экспорта маршрутов из VRF данного экземпляра BGP в другие VRF.

   - В блоке **Route Target для импорта** добавьте с помощью кнопки **Добавить** одно или несколько значений Route Target (RT) для импорта маршрутов в VRFданного экземпляра BGP из других VRF.

     Отдельные значения записей Route Target для параметров **Route Target для экспорта** и **Route Target для импорта** записываются в одном из двух форматов:

     - Номер AS (число от 0 до 4294967295) : идентификатор (число от 0 до 65535). Пример: `100:3000`.

     - IPv4-адрес : идентификатор (число от 0 до 65535). Пример: `6.6.6.6:77`.

   - Включите переключатель **Экспортировать маршруты**, если необходимо экспортировать маршруты из из VRF данного экземпляра BGP.

   - Включите переключатель **Импортировать маршруты**, если необходимо импортировать маршруты в VRF данного экземпляра BGP.

   - В списках **Карта маршрутизации для экспортируемых маршрутов** и **Карта маршрутизации для импортируемых маршрутов** выберите созданные карты маршрутизации для экспортируемых и импортируемых маршрутов.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, или **Отмена**, чтобы отменить изменения.

Обмен маршрутами по протоколу OSPF

Kaspersky SD-WAN поддерживает протокол динамической маршрутизации OSPF (Open Shortest Path First) для обмена маршрутной информацией между устройствами CPE и внешними сетевыми устройствами. При настройке протокола OSPF вы можете использовать OSPF-области (англ. OSPF areas) и OSPF-интерфейсы.

Настройка основных параметров OSPF

Вы можете настроить основные параметры OSPF в шаблоне CPE или на устройстве CPE. Основные параметры OSPF, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

Чтобы настроить основные параметры OSPF:

1. Перейдите к настройке основных параметров OSPF одним из следующих способов:

   - Если вы хотите настроить основные параметры OSPF в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **OSPF**.

   - Если вы хотите настроить основные параметры OSPF на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **OSPF** и установите флажок **Переопределить**.

   По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются параметры OSPF.

2. В раскрывающемся списке **OSPF** выберите **Включено**. Значение по умолчанию: **Выключено**.

3. В поле **Router ID** введите IPv4-адрес, который вы хотите назначить идентификатору маршрутизатора (англ. router ID) устройства CPE.

4. В поле **Максимум путей** введите максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 16.

5. Если вы хотите использовать устройство CPE как пограничный маршрутизатор (англ. Area Border Router, ABR), в раскрывающемся списке **Тип ABR** выберите одну из следующих имплементаций:

   - **IBM** – имплементация по умолчанию.

   - **CISCO**.

   - **SHORTCUT**.

   - **STANDARD**.

6. В поле **Пропускная способность для автоопределения стоимости** введите контрольное значение пропускной способности для подсчета стоимости соединений на устройстве CPE. Диапазон значений: от 1 до 4 294 967.

7. Если вы хотите перевести OSPF-интерфейсы устройства CPE в пассивный режим, установите флажок **Пассивный интерфейс по умолчанию**. В пассивном режиме OSPF-интерфейсы не обмениваются пакетами трафика. Этот флажок снят по умолчанию.

8. Если вы хотите вести журнал OSPF, установите флажок **Журнал изменений смежности**. Вы можете установить флажок **Подробный журнал**, чтобы вести более подробный журнал OSPF. По умолчанию флажки сняты.

9. Если вы хотите настроить перераспределение маршрутов в OSPF, в блоке **Перераспределение маршрутов** выполните следующие действия:

   a. Установите флажки рядом с типами маршрутов:

   - **BGP** – перераспределять BGP-маршруты.
   - **Connected** – перераспределять маршруты, напрямую подключенные к сетевым интерфейсам устройства CPE.
   - **Kernel** – перераспределять Kernel-маршруты, генерируемые операционной системой устройства CPE.
   - **Статический** – перераспределять статические маршруты.

   По умолчанию флажки сняты.

   b. В раскрывающемся списке **Карта маршрутизации** выберите созданную карту маршрутизации для перераспределяемых маршрутов.

   c. В поле **Метрика** введите метрику перераспределяемых маршрутов. Диапазон значений: от 0 до 16 777 214.

   d. В раскрывающемся списке **Тип метрики** выберите тип метрики:

   - **Type 1** (или "внутренняя метрика").
   - **Type 2** (или "внешняя метрика").

   e. Установите флажок **Фильтрация** и в раскрывающемся списке **Список управления доступом** выберите созданный список управления доступом для перераспределяемых маршрутов. Этот флажок снят по умолчанию.

10. В поле **Метрика по умолчанию** введите метрику по умолчанию OSPF-маршрутов. Диапазон значений: от 0 до 16 777 214.

11. Если вы хотите настроить анонсирование устройством CPE маршрута по умолчанию 0.0.0.0/0 OSPF-соседям, выполните следующие действия:

    a. Установите флажок **Маршрут по умолчанию**. Этот флажок снят по умолчанию.

    b. Установите флажок **Всегда**, чтобы всегда анонсировать маршрут по умолчанию 0.0.0.0/0, даже если он отсутствует в таблице маршрутизации устройства CPE. Этот флажок снят по умолчанию.

    c. В раскрывающемся списке **Тип метрики** выберите тип метрики для маршрута по умолчанию 0.0.0.0/0:

    - **Type 1**.
    - **Type 2**.

    d. В поле **Метрика** введите метрику маршрута по умолчанию 0.0.0.0/0. Диапазон значений: от 0 до 16 777 214.

    e. В раскрывающемся списке **Карта маршрутизации** выберите созданную карту маршрутизации для маршрута по умолчанию 0.0.0.0/0.

12. В поле **Дистанция** введите административную дистанцию для всех OSPF-маршрутов. Чем ниже значение административной дистанции, указанное для протокола, тем выше приоритет его маршрутов. Например, если вы хотите, чтобы маршрутам, полученным из протокола OSPF, всегда отдавалось предпочтение по отношению к маршрутам, полученным из протокола BGP, укажите административную дистанцию 1 для OSPF и 2 для BGP. Диапазон значений: от 1 до 255.

13. Если вы хотите настроить административные дистанции для отдельных OSPF-маршрутов, выполните следующие действия:

    a. Установите флажок **Дистанция OSPF**. Этот флажок снят по умолчанию.

    b. В поле **Внешняя** введите административную дистанцию для маршрутов из внешних OSPF-доменов или протоколов маршрутизации. Диапазон значений: от 1 до 255.

    c. В поле **Между областями** введите административную дистанцию для маршрутов из разных OSPF-областей одного OSPF-домена. Диапазон значений: от 1 до 255.

    d. В поле **Внутри области** введите административную дистанцию для маршрутов из одной OSPF-области. Диапазон значений: от 1 до 255.

14. Если вы хотите включить перезагрузку Graceful restart на устройстве CPE, выполните следующие действия:

    a. Установите флажок **Graceful restart**. Этот флажок снят по умолчанию.

    b. В поле **Grace period (сек.)** введите время в секундах, в течение которого устройство CPE анонсирует намерение выполнить перезагрузку OSPF-соседям. Диапазон значений: от 1 до 1800.

15. Если вы хотите настроить таймеры для вычислений алгоритма Shortest Path First (SPF, далее SPF-алгоритм), выполните следующие действия:

    a. Установите флажок **Таймеры ограничения частоты SPF**. Этот флажок снят по умолчанию.

    b. В поле **Задержка (мс)** введите время задержки в миллисекундах перед началом вычислений SPF-алгоритма. Диапазон значений: от 0 до 600 000.

    c. В поле **Изначальное время удержания (мс)** введите минимальное время удержания в миллисекундах между двумя вычислениями SPF-алгоритма. Диапазон значений: от 0 до 600 000.

    d. В поле **Максимальное время удержания (мс)** введите максимальное время удержания в миллисекундах между двумя вычислениями SPF-алгоритма. Диапазон значений: от 0 до 600 000.

16. Если вы хотите настроить анонсирование устройством CPE состояния соединения (англ. Link State Advertisement, далее также LSA) OSPF-соседям, выполните следующие действия:

    a. Установите флажок **По требованию администратора**, чтобы устройство CPE использовало максимальную метрику в анонсах состояния соединения OSPF-соседям.

    b. Если вы хотите указать время, в течение которого устройство CPE использует максимальную метрику в анонсах состояния соединения OSPF-соседям при запуске или перезапуске протокола OSPF, выполните следующие действия:

        1. Установите флажок **При запуске**. Этот флажок снят по умолчанию.

        2. В поле **Таймер (сек.)** введите время в секундах. Диапазон значений: от 5 до 86 400.

    c. Если вы хотите указать время, в течение которого устройство CPE использует максимальную метрику в анонсах состояния соединения OSPF-соседям при выключении протокола OSPF, выполните следующие действия:

        1. Установите флажок **При выключении**. Этот флажок снят по умолчанию.

        2. В поле **Таймер (сек.)** введите время в секундах. Диапазон значений: от 5 до 100.

17. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с OSPF-областями

Вы можете посмотреть таблицу OSPF-областей в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы OSPF-областей в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **OSPF** → **OSPF-области**.

- Для просмотра таблицы OSPF-областей на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **CPE**, нажать на устройство CPE и выбрать вкладку **OSPF** → **OSPF-области**.

Информация об OSPF-областях отображается в следующих столбцах таблицы:

- **OSPF-область** – идентификатор OSPF-области в формате IPv4-адреса или целого числа.

- **Тип области** – тип тупиковой OSPF-области:

    - **Stub**.

    - **Stub NO-SUMMARY**.

    - **NSSA**.

    - **NSSA NO-SUMMARY**.

    Значение отображается только для тупиковых областей.

- **OSPF-диапазоны** – диапазоны OSPF.
- **Управление** – действия, которые можно выполнить с OSPF-областью.

Создание OSPF-области

Вы можете создать OSPF-область в шаблоне CPE или на устройстве CPE. OSPF-область, созданная в шаблоне CPE, автоматически создается на всех устройствах CPE, к которым применен шаблон CPE.

Чтобы создать OSPF-область:

1. Перейдите к созданию OSPF-области одним из следующих способов:
   - Если вы хотите создать OSPF-область в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **OSPF** → **OSPF-области**.
   - Если вы хотите создать OSPF-область на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **OSPF** → **OSPF-области** и установите флажок **Переопределить**.

   Отобразится таблица OSPF-областей.
2. Нажмите на кнопку **+ OSPF-область**.
3. В открывшемся окне в поле **OSPF-область** введите идентификатор OSPF-области в формате IPv4-адреса или целого числа.
4. Если вы хотите сделать OSPF-область тупиковой (англ. stub area), выполните следующие действия:
   a. Установите флажок **Stub**. Этот флажок снят по умолчанию.
   b. В раскрывающемся списке **Тип области** выберите тип тупиковой OSPF-области:
      - **Stub**.
      - **Stub NO-SUMMARY**.
      - **NSSA**.
      - **NSSA NO-SUMMARY**.
   c. Если в раскрывающемся списке **Тип области** вы выбрали **NSSA** или **NSSA NO-SUMMARY**, при необходимости запретить анонсирование маршрута по умолчанию 0.0.0.0/0 в NSSA-область установите флажок **Подавлять FA в NSSA**. Этот флажок снят по умолчанию.
   d. В поле **Стоимость по умолчанию** введите метрику маршрута по умолчанию или суммированных маршрутов. Диапазон значений: от 0 до 16 777 215.
5. Если вы хотите использовать метод кратчайшего маршрута (англ. shortcut) при выполнении вычислений SPF-алгоритма, установите флажок **Сокращенные маршруты**. Этот флажок снят по умолчанию.

6. В раскрывающемся списке **Аутентификация** выберите метод аутентификации в OSPF:

   - **Хеш-функция** – использовать MD5-алгоритм.
   - **Пароль** – использовать незашифрованный пароль. Этот метод аутентификации является менее надежным по сравнению с MD5-алгоритмом, однако может обеспечить аутентификацию при использовании в доверенном сетевом окружении.

7. Если вы хотите указать диапазоны OSPF, выполните следующие действия:

   a. В блоке **OSPF-диапазоны** нажмите на кнопку **+ Диапазон**.

   b. В поле **Диапазон** введите IPv4-префикс маршрутов.

   c. В раскрывающемся списке **Действие** выберите действие, которое выполняется с маршрутами:

      - **Анонсировать** – анонсировать маршруты по протоколу OSPF. Это значение выбрано по умолчанию.
      - **Не анонсировать** – не анонсировать маршруты по протоколу OSPF.
      - **Заменять** – заменять IPv4-префикс маршрутов на указанный IPv4-префикс, после чего анонсировать в OSPF. При выборе этого значения в поле **Заменять** введите IPv4-префикс маршрутов.

   d. Если в раскрывающемся списке **Действие** вы выбрали **Анонсировать** или **Заменять**, в поле **Стоимость** введите метрику маршрутов. Диапазон значений: от 0 до 16 777 215.

   Диапазон OSPF будет указан и отобразится в блоке **OSPF-диапазоны**. Вы можете указать несколько диапазонов OSPF и удалить диапазоны OSPF. Для удаления диапазона OSPF нажмите рядом с ним на значок удаления ✕.

8. Если вы хотите соединить OSPF-область с другой OSPF-областью через транзитную OSPF-область, укажите виртуальное соединение:

   a. В блоке **Виртуальные соединения** нажмите на кнопку **+ Виртуальное соединение**.

   b. В поле **Адрес** введите IPv4-адрес сетевого интерфейса маршрутизатора в транзитной области.

   Виртуальное соединение будет указано и отобразится в блоке **OSPF-диапазоны**. Вы можете указать несколько виртуальных соединений и удалить виртуальные соединения. Для удаления виртуального соединения нажмите рядом с ним на значок удаления ✕.

9. Если вы хотите настроить фильтрацию маршрутов для OSPF-области, в блоке **Фильтрация** выполните следующие действия:

   a. Выберите созданные списки управления доступом:

      1. В раскрывающемся списке **Список экспорта** выберите список управления доступом для маршрутов, которые анонсируются из OSPF-области в другие OSPF-области.

      2. В раскрывающемся списке **Список импорта** выберите список управления доступом для маршрутов, которые анонсируются из других OSPF-областей в OSPF-область.

   b. Выберите созданные списки префиксов:

      1. В раскрывающемся списке **Исходящий список фильтрации** выберите список префиксов для маршрутов, которые анонсируются из OSPF-области в другие OSPF-области.

      2. В раскрывающемся списке **Входящий список фильтрации** выберите список префиксов для маршрутов, которые анонсируются из других OSPF-областей в OSPF-область.

10. Нажмите на кнопку **Сохранить**.

    OSPF-область будет создана и отобразится в таблице.

11. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение OSPF-области

Вы можете изменить OSPF-область в шаблоне CPE или на устройстве. OSPF-область, измененная в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить OSPF-область:

1. Перейдите к изменению OSPF-области одним из следующих способов:

   - Если вы хотите изменить OSPF-область в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **OSPF** → **OSPF-области**.

   - Если вы хотите изменить OSPF-область на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **OSPF** → **OSPF-области** и установите флажок **Переопределить**.

   Отобразится таблица OSPF-областей.

2. Нажмите на кнопку **Изменить** рядом с OSPF-областью, которую вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры OSPF-области. Описание параметров см. в инструкции по созданию OSPF-области.

4. Нажмите на кнопку **Сохранить**.

   OSPF-область будет изменена и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление OSPF-области

Вы можете удалить OSPF-область в шаблоне CPE или на устройстве CPE. OSPF-область, удаленная в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE.

Удаленные OSPF-области невозможно восстановить.

Чтобы удалить OSPF-область:

1. Перейдите к удалению OSPF-области одним из следующих способов:

   - Если вы хотите удалить OSPF-область в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **OSPF** → **OSPF-области**.

   - Если вы хотите удалить OSPF-область на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **OSPF** → **OSPF-области** и установите флажок **Переопределить**.

   Отобразится таблица OSPF-областей.

2. Нажмите на кнопку **Удалить** рядом с OSPF-областью, которую вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   OSPF-область будет удалена и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с OSPF-интерфейсами

Вы можете посмотреть таблицу OSPF-интерфейсов в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы OSPF-интерфейсов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **OSPF** → **OSPF-интерфейсы**.

- Для просмотра таблицы OSPF-интерфейсов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **CPE**, нажать на устройство CPE и выбрать вкладку **OSPF** → **OSPF-интерфейсы**.

Информация об OSPF-интерфейсах отображается в следующих столбцах таблицы:

- **Интерфейс** – сетевой интерфейс, который используется как OSPF-интерфейс.
- **OSPF-область** – идентификатор OSPF-области, к которой относится OSPF-интерфейс.
- **Аутентификация** – метод аутентификации.
- **Тип сети** – тип сети, к которой подключен OSPF-интерфейс.
- **Управление** – действия, которые можно выполнить с OSPF-интерфейсом.

Создание OSPF-интерфейса

Вы можете создать OSPF-интерфейс в шаблоне CPE или на устройстве CPE. OSPF-интерфейс, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать OSPF-интерфейс:

1. Перейдите к созданию OSPF-интерфейса одним из следующих способов:

   - Если вы хотите создать OSPF-интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **OSPF** → **OSPF-интерфейсы**.
   - Если вы хотите создать OSPF-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **OSPF** → **OSPF-интерфейсы** и установите флажок **Переопределить**.

   Отобразится таблица OSPF-интерфейсов.

2. Нажмите на кнопку **+ OSPF-интерфейс**.
3. В открывшемся окне в раскрывающемся списке **Интерфейс** выберите созданный сетевой интерфейс, который вы хотите использовать как OSPF-интерфейс.
4. В поле **OSPF-область** введите идентификатор OSPF-области, к которой относится OSPF-интерфейс, в формате IPv4-адреса или целого числа.

5. Если вы хотите настроить аутентификацию в OSPF, выполните следующие действия:

   a. В раскрывающемся списке **Аутентификация** выберите метод аутентификации:

      - **Хеш-функция** – использовать MD5-алгоритм.
      - **Пароль** – использовать незашифрованный пароль. Этот метод аутентификации является менее надежным по сравнению с MD5-алгоритмом, однако может обеспечить аутентификацию при использовании в доверенном сетевом окружении. При выборе этого значения в поле **Пароль** введите пароль для аутентификации.

   b. Если в раскрывающемся списке **Аутентификация** вы выбрали **Хеш-функция**, выполните следующие действия:

      1. В поле **ID ключа** введите MD5-хеш. Диапазон значений: от 1 до 255.
      2. В поле **Ключ** введите MD5-ключ.

6. В поле **Стоимость** введите метрику OSPF-интерфейса. Диапазон значений: от 1 до 65 535.
7. В раскрывающемся списке **Тип сети** выберите тип сети, к которой подключен OSPF-интерфейс:

   - **Broadcast**.
   - **Non-broadcast**.
   - **Point-to-multipoint**.
   - **Point-to-point**.

8. В поле **Приоритет** введите приоритет OSPF-интерфейса. Чем выше введенное значение, тем выше приоритет OSPF-интерфейса.

   OSPF-интерфейс с наивысшим приоритетом становится выделенным маршрутизатором (англ. designated router) в сегменте сети. OSPF-интерфейс со вторым по величине приоритетом становится резервным выделенным маршрутизатором (англ. backup designated router).

9. Если вы хотите перевести OSPF-интерфейс в пассивный режим, установите флажок **Пассивный интерфейс**. В пассивном режиме OSPF-интерфейсы не обмениваются пакетами трафика.
10. Если вы хотите использовать протокол BFD для обнаружения потери связности, установите флажок **BFD**. Этот флажок снят по умолчанию.
11. Если вы хотите настроить OSPF-таймеры, выполните следующие действия:

    a. Установите флажок **OSPF-таймеры**. Этот флажок снят по умолчанию.

    b. В поле **Hello (сек.)** введите интервал времени в секундах для отправки OSPF-интерфейсом контрольных пакетов OSPF-соседям. Диапазон значений: от 1 до 65 535.

    c. В поле **Dead (сек.)** введите интервал времени в секундах для получения OSPF-интерфейсом контрольных пакетов от OSPF-соседей. Если в течение указанного времени от OSPF-соседа не поступает контрольных пакетов, OSPF-интерфейс считает OSPF-соседа недоступным. Диапазон значений: от 1 до 65 535.

12. В поле **Интервал повторной передачи (сек.)** введите интервал времени в секундах для повторной отправки LSA-пакетов (Link State Advertisement) OSPF-соседям, которые находятся за OSPF-интерфейсом. Диапазон значений от 1 до 65 535. Более подробную информацию можно получить из стандарта RFC 2328 (параметр – `RxmtInterval`).

13. В поле **Задержка при передаче (сек.)** введите предполагаемое время в секундах, необходимое для отправки LSU-пакета (Link State Update) через OSPF-интерфейс. Диапазон значений от 1 до 65 535. Более подробную информацию можно получить из стандарта RFC 2328 (параметр – `InfTransDelay`).

14. Нажмите на кнопку **Создать**.

    OSPF-интерфейс будет создан и отобразится в таблице.

15. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение OSPF-интерфейса

Вы можете изменить OSPF-интерфейс в шаблоне CPE или на устройстве CPE. OSPF-интерфейс, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить OSPF-интерфейс:

1. Перейдите к изменению OSPF-интерфейса одним из следующих способов:

   - Если вы хотите изменить OSPF-интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **OSPF → OSPF-интерфейсы**.

   - Если вы хотите изменить OSPF-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **OSPF → OSPF-интерфейсы** и установите флажок **Переопределить**.

   Отобразится таблица OSPF-интерфейсов.

2. Нажмите на кнопку **Изменить** рядом с OSPF-интерфейсом, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры OSPF-интерфейса. Описание параметров см. в инструкции по созданию OSPF-интерфейса.

4. Нажмите на кнопку **Сохранить**.

   OSPF-интерфейс будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление OSPF-интерфейса

Вы можете удалить OSPF-интерфейс в шаблоне CPE или на устройстве CPE. OSPF-интерфейс, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE.

Удаленные интерфейсы невозможно восстановить.

Чтобы удалить OSPF-интерфейс:

1. Перейдите к удалению OSPF-интерфейса одним из следующих способов:

   - Если вы хотите удалить OSPF-интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **OSPF** → **OSPF-интерфейсы**.
   - Если вы хотите удалить OSPF-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **OSPF** → **OSPF-интерфейсы** и установите флажок **Переопределить**.

   Отобразится таблица OSPF-интерфейсов.

2. Нажмите на кнопку **Удалить** рядом с OSPF-интерфейсом, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   OSPF-интерфейс будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Обнаружение ошибок маршрутизации с помощью протокола BFD

Kaspersky SD-WAN поддерживает протокол BFD (Bidirectional Forwarding Detection) для быстрого (в пределах одной секунды) обнаружения проблем с сетевой связностью на соединениях. При обнаружении проблемы BFD передает информацию о ней с плоскости передачи данных на плоскость управления сетью.

Между BFD-соседями устанавливается BFD-сессия, в рамках которой они обмениваются контрольными пакетами для обнаружения проблем с сетевой связностью. При возникновении проблем с сетевой связностью происходит разрыв BFD-сессии на интерфейсе SD-WAN устройства CPE, после чего перестраиваются таблицы маршрутизации.

Вы можете посмотреть таблицу BFD-соседей в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы BFD-соседей в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **BFD**.
- Для просмотра таблицы BFD-соседей на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **CPE**, нажать на устройство CPE и выбрать вкладку **BFD**.

Информация о BFD-соседях отображается в следующих столбцах таблицы:

- **Имя** – имя BFD-соседа
- **IP-адрес** – IPv4-адрес BFD-соседа.
- **Интервал передачи (мс)** – интервал времени в миллисекундах для отправки устройством CPE контрольных пакетов BFD-соседу.
- **Интервал получения (мс)** – интервал времени в миллисекундах для получения устройством CPE контрольных пакетов от BFD-соседа. Если в течение указанного времени от BFD-соседа не поступает контрольных пакетов, устройство CPE считает BFD-соседа недоступным.
- **Множитель** – множитель интервала времени для отправки контрольных пакетов, указанного в параметрах BFD-соседа. Этот множитель определяет время в миллисекундах, в течение которого устройство CPE ожидает получения контрольных пакетов от BFD-соседа. Если в течение этого времени от BFD-соседа не поступает контрольных пакетов, устройство CPE анонсирует проблему с сетевой связностью.
- **Управление** – действия, которые можно выполнить с BFD-соседом.

Включение и выключение протокола BFD

Вы можете включить или выключить протокол BFD в шаблоне CPE или на устройстве CPE. Протокол BFD, включенный или выключенный в шаблоне CPE, автоматически включается или выключается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы включить или выключить протокол BFD:

1. Перейдите к включению или выключению протокола BFD одним из следующих способов:

   - Если вы хотите включить или выключить протокол BFD в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BFD**.

   - Если вы хотите включить или выключить протокол BFD на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **BFD** и установите флажок **Переопределить**.

   Отобразится таблица BFD-соседей.

2. В раскрывающемся списке **BFD** выберите одно из следующих значений:

   - **Включено**.

   - **Выключено**. Это значение выбрано по умолчанию.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Создание BFD-соседа

Вы можете создать BFD-соседа в шаблоне CPE или на устройстве CPE. BFD-сосед, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE. Перед созданием BFD-соседа вам нужно включить протокол BFD.

Чтобы создать BFD-соседа:

1. Перейдите к созданию BFD-соседа одним из следующих способов:

   - Если вы хотите создать BFD-соседа в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BFD**.

   - Если вы хотите создать BFD-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **BFD** и установите флажок **Переопределить**.

   Отобразится таблица BFD-соседей.

2. Нажмите на кнопку **+ BFD-сосед**.

3. В открывшемся окне в поле **Имя** введите имя BFD-соседа. Максимальная длина имени: 255 символов.

4. В поле **IP-адрес** введите IPv4-адрес BFD-соседа.

5. В поле **Интервал передачи (мс)** введите интервал времени в миллисекундах для отправки устройством CPE контрольных пакетов BFD-соседу. Диапазон значений: от 60 до 10000.

6. В поле **Интервал получения (мс)** введите интервал времени в миллисекундах для получения устройством CPE контрольных пакетов от BFD-соседа. Если в течение указанного времени от BFD-соседа не поступает контрольных пакетов, устройство CPE считает этого BFD-соседа недоступным. Диапазон значений: от 60 до 10000.

7. В поле **Множитель** введите множитель интервала времени для отправки контрольных пакетов, указанного в параметрах BFD-соседа. Этот множитель определяет время в миллисекундах, в течение которого устройство CPE ожидает получения контрольных пакетов от BFD-соседа. Если в течение этого времени от BFD-соседа не поступает контрольных пакетов, устройство CPE анонсирует проблему с сетевой связностью. Диапазон значений: от 2 до 255.

   Например, если интервал времени для отправки контрольных пакетов в параметрах BFD-соседа равен 200 миллисекунд, и вы указываете множитель 2, по истечении 400 миллисекунд устройство CPE анонсирует проблему с сетевой связностью при отсутствии контрольных пакетов от BFD-соседа.

8. Нажмите на кнопку **Создать**.

   BFD-сосед будет создан и отобразится в таблице.

9. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение BFD-соседа

Вы можете изменить BFD-соседа в шаблоне CPE или на устройстве CPE. BFD-сосед, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить BFD-соседа:

1. Перейдите к изменению BFD-соседа одним из следующих способов:

   - Если вы хотите изменить BFD-соседа в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BFD**.

   - Если вы хотите изменить BFD-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **BFD** и установите флажок **Переопределить**.

   Отобразится таблица BFD-соседей.

2. Нажмите на кнопку **Изменить** рядом с BFD-соседом, которого вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры BFD-соседа. Описание параметров см. в инструкции по созданию BFD-соседа.

4. Нажмите на кнопку **Сохранить**.

   BFD-сосед будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление BFD-соседа

Вы можете удалить BFD-соседа в шаблоне CPE или на устройстве CPE. BFD-сосед, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE.

Удаленных BFD-соседей невозможно восстановить.

Чтобы удалить BFD-соседа:

1. Перейдите к удалению BFD-соседа одним из следующих способов:

   - Если вы хотите удалить BFD-соседа в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **BFD**.
   - Если вы хотите удалить BFD-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **BFD** и установите флажок **Переопределить**.

   Отобразится таблица BFD-соседей.

2. Нажмите на кнопку **Удалить** рядом с BFD-соседом, которого вы хотите удалить.

3. В открывшемся окне нажмите на кнопку **Удалить**.

   BFD-сосед будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Обеспечение высокой доступности с помощью протокола VRRP

Kaspersky SD-WAN поддерживает протокол VRRP (Virtual Router Redundancy Protocol) для объединения сетевых интерфейсов нескольких устройств CPE в виртуальные маршрутизаторы. Когда сетевые интерфейсы объединены в виртуальный маршрутизатор, они используют общий виртуальный IP-адрес. Один сетевой интерфейс является основным, а другие – второстепенными. Виртуальный IP-адрес назначается основному сетевому интерфейсу.

Сетевые интерфейсы в виртуальном маршрутизаторе обмениваются контрольными пакетами, чтобы определить, какие сетевые интерфейсы выходят из строя. Если основной сетевой интерфейс выходит из строя, выбирается новый основной сетевой интерфейс, которому назначается виртуальный IP-адрес. Трафик, передающийся на виртуальный IP-адрес через вышедший из строя сетевой интерфейс, автоматически начинает передаваться через новый основной сетевой интерфейс.

Вы можете создавать экземпляры VRRP, чтобы объединять сетевые интерфейсы в виртуальные маршрутизаторы. При создании экземпляра VRRP вам нужно указать сетевой интерфейс, идентификатор виртуального маршрутизатора Virtual Router ID (VRID) и виртуальный IP-адрес. Сетевые интерфейсы объединяются в виртуальный маршрутизатор, если в созданных для них экземплярах VRRP указан одинаковый идентификатор виртуального маршрутизатора и виртуальный IP-адрес.

При необходимости синхронно изменить основной сетевой интерфейс в нескольких виртуальных маршрутизаторах можно создать группы экземпляров VRRP. Если основной сетевой интерфейс изменяется в одном из экземпляров VRRP, это изменение происходит в остальных экземплярах VRRP в группе экземпляров VRRP.

Включение и выключение протокола VRRP

Вы можете включить или выключить протокол VRRP в шаблоне CPE или на устройстве CPE. Протокол VRRP, включенный и выключенный в шаблоне CPE, автоматически включается или выключается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы включить или выключить протокол VRRP:

1. Перейдите к включению или выключению протокола VRRP одним из следующих способов:

   - Если вы хотите включить или выключить протокол VRRP в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRRP → Экземпляры VRRP**.

   - Если вы хотите включить или выключить протокол VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **VRRP → Экземпляры VRRP** и установите флажок **Переопределить**.

   Отобразится таблица экземпляров VRPP.

2. В раскрывающемся списке **VRRP** выберите одно из следующих значений:

   - **Включено**.

   - **Выключено**. Это значение выбрано по умолчанию.

   При включении протокола VRRP вам нужно создать хотя бы один экземпляр VRRP.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с экземплярами VRRP

Вы можете посмотреть таблицу экземпляров VRRP в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы экземпляров VRRP в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **VRRP → Экземпляры VRRP**.
- Для просмотра таблицы экземпляров VRRP на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **VRRP → Экземпляры VRRP**.

Информация об экземплярах VRRP отображается в следующих столбцах таблицы:

- **Имя** – имя экземпляра VRRP.
- **VRID** – идентификатор виртуального маршрутизатора.
- **Интерфейс** – сетевой интерфейс, который был добавлен в виртуальный маршрутизатор.
- **VIP** – виртуальный IP-адрес, назначенный сетевому интерфейсу.
- **Состояние** – роль сетевого интерфейса:
  - **Backup** – резервный сетевой интерфейс.
  - **Master** – основной сетевой интерфейс.
- **Приоритет** – приоритет сетевого интерфейса. Чем выше введенное значение, тем выше приоритет. При прекращении работы основного сетевого интерфейса его заменяет резервный сетевой интерфейс с наивысшим приоритетом. Если при выборе нового основного сетевого интерфейса все резервные сетевые интерфейсы имеют одинаковый приоритет, новый основной сетевой интерфейс выбирается случайно.
- **Интервал оповещения (сек.)** – интервал времени в секундах для отправки сетевым интерфейсом контрольных пакетов другим сетевым интерфейсам.
- **Nopreempt** – роль сетевого интерфейса, ставшего основным, изменяется, если прежний основной сетевой интерфейс восстанавливает работу:
  - **Да**.
  - **Нет**.
- **Управление** – действия, которые можно выполнить с экземпляром VRRP.

Создание экземпляра VRRP

Вы можете создать экземпляр VRRP в шаблоне CPE или на устройстве CPE. Экземпляр VRRP, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать экземпляр VRRP:

1. Перейдите к созданию экземпляра VRRP одним из следующих способов:

   - Если вы хотите создать экземпляр VRRP в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRRP** → **Экземпляры VRRP**.

   - Если вы хотите создать экземпляр VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **VRRP** → **Экземпляры VRRP** и установите флажок **Переопределить**.

   Отобразится таблица экземпляров VRPP.

2. Нажмите на кнопку **+ Экземпляр VRRP**.

3. В открывшемся окне в поле **Имя** введите имя экземпляра VRRP. Максимальная длина имени: 16 символов.

4. В поле **VRID** введите идентификатор виртуального маршрутизатора. Вам нужно указать одинаковый идентификатор при создании экземпляров VRRP для всех сетевых интерфейсов, которые вы хотите объединить в виртуальный маршрутизатор. Диапазон значений: от 1 до 255.

5. В раскрывающемся списке **Интерфейс** выберите созданный сетевой интерфейс, который вы хотите добавить в виртуальный маршрутизатор.

6. В поле **VIP** введите виртуальный IP-адрес, который вы хотите назначить сетевому интерфейсу. Вам нужно назначить одинаковый виртуальный IP-адрес всем сетевым интерфейсам, которые вы хотите объединить в виртуальный маршрутизатор.

7. В раскрывающемся списке **Состояние** выберите роль сетевого интерфейса:

   - **Backup** – резервный сетевой интерфейс. Это значение выбрано по умолчанию.

   - **Master** – основной сетевой интерфейс.

8. В поле **Приоритет** введите приоритет сетевого интерфейса. Чем выше введенное значение, тем выше приоритет. При прекращении работы основного сетевого интерфейса его заменяет резервный сетевой интерфейс с наивысшим приоритетом. Если при выборе нового основного сетевого интерфейса все резервные сетевые интерфейсы имеют одинаковый приоритет, новый основной сетевой интерфейс выбирается случайно. Диапазон значений: от 1 до 255. Значение по умолчанию: `100`.

9. В поле **Интервал оповещения (сек.)** введите интервал времени в секундах для отправки сетевым интерфейсом контрольных пакетов другим сетевым интерфейсам. Диапазон значений: от 1 до 60. Значение по умолчанию: `5`.

10. При необходимости не изменять роль резервного сетевого интерфейса, ставшего основным, если прежний основной сетевой интерфейс восстанавливает работу, установите флажок **Nopreempt**. Этот флажок снят по умолчанию.

11. Если вы хотите настроить unicast-отправку контрольных пакетов сетевым интерфейсом, выполните следующие действия:

    a. Установите флажок **Unicast**. Этот флажок снят по умолчанию.

    b. В поле **IP источника unicast** введите IP-адрес сетевого интерфейса источника для отправки контрольных пакетов.

    c. В поле **IP unicast-соседа** введите IP-адрес сетевого интерфейса назначения для отправки контрольных пакетов.

    По умолчанию сетевой интерфейс использует multicast-отправку контрольных пакетов.

12. Если вы хотите использовать пароль для аутентификации контрольных пакетов на сетевом интерфейсе, выполните следующие действия:

    a. Установите флажок **Аутентификация**. Этот флажок снят по умолчанию.

    b. В отобразившемся поле введите пароль. Максимальная длина пароля: 16 символов. Вам нужно указать одинаковый пароль для всех сетевых интерфейсов, которые вы хотите объединить в виртуальный маршрутизатор. Вы можете просмотреть введенный пароль, нажав на значок просмотра .

13. Нажмите на кнопку **Создать**.

    Экземпляр VRRP будет создан и отобразится в таблице.

14. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение экземпляра VRRP

Вы можете изменить экземпляр VRRP в шаблоне CPE или на устройстве CPE. Экземпляр VRRP, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете изменить на устройстве CPE экземпляр VRRP, унаследованный из шаблона CPE.

Чтобы изменить экземпляр VRRP:

1. Перейдите к изменению экземпляра VRRP одним из следующих способов:

    - Если вы хотите изменить экземпляр VRRP в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRRP → Экземпляры VRRP**.

    - Если вы хотите изменить экземпляр VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **VRRP → Экземпляры VRRP** и установите флажок **Переопределить**.

    Отобразится таблица экземпляров VRPP.

2. Нажмите на кнопку **Изменить** рядом с экземпляром VRRP, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры экземпляра VRRP. Описание параметров см. в инструкции по созданию экземпляра VRRP.

4. Нажмите на кнопку **Сохранить**.

   Экземпляр VRRP будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление экземпляра VRRP

Вы можете удалить экземпляр VRRP в шаблоне CPE или на устройстве CPE. Экземпляр VRRP, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете удалить на устройстве CPE экземпляр VRRP, унаследованный из шаблона CPE.

Удаленные экземпляры VRRP невозможно восстановить.

Чтобы удалить экземпляр VRRP:

1. Перейдите к удалению экземпляра VRRP одним из следующих способов:

   - Если вы хотите удалить экземпляр VRRP в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRRP → Экземпляры VRRP**.

   - Если вы хотите удалить экземпляр VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **VRRP → Экземпляры VRRP** и установите флажок **Переопределить**.

   Отобразится таблица экземпляров VRPP.

2. Нажмите на кнопку **Удалить** рядом с экземпляром VRRP, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Экземпляр VRRP будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с группами экземпляров VRRP

Вы можете посмотреть таблицу групп экземпляров VRRP в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы групп экземпляров VRRP в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **VRRP → Группы экземпляров VRRP**.

- Для просмотра таблицы групп экземпляров VRRP на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **VRRP → Группы экземпляров VRRP**.

Информация о группах экземпляров VRRP отображается в следующих столбцах таблицы:

- **Имя** – имя группы экземпляров VRRP.
- **Экземпляры VRRP** – экземпляры VRRP, которые были добавлены в группу экземпляров VRRP.
- **Управление** – действия, которые можно выполнить с группой экземпляров VRRP.

Создание группы экземпляров VRRP

Вы можете создать группу экземпляров VRRP в шаблоне CPE или на устройстве CPE. Группа экземпляров VRRP, созданная в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать группу экземпляров VRRP:

1. Перейдите к созданию группы экземпляров VRRP одним из следующих способов:

   - Если вы хотите создать группу экземпляров VRRP в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRRP → Группы экземпляров VRRP**.
   - Если вы хотите создать группу экземпляров VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **VRRP → Группы экземпляров VRRP** и установите флажок **Переопределить**.

   Отобразится таблица групп экземпляров VRRP.

2. Нажмите на кнопку **+ Группа экземпляров VRRP**.
3. В открывшемся окне в поле **Имя** введите имя группы экземпляров VRRP. Максимальная длина имени: 16 символов. Значение по умолчанию: `1`.
4. В раскрывающемся списке **Экземпляры VRRP** выберите созданный экземпляр VRRP, который вы хотите добавить в группу экземпляров VRRP.

   Экземпляр VRRP будет добавлен и отобразится в нижней части окна. Вы можете добавить несколько экземпляров VRRP и удалить экземпляры VRRP. Для удаления экземпляра VRRP нажмите рядом с ним на кнопку **Удалить**.

5. Нажмите на кнопку **Создать**.

   Группа экземпляров VRRP будет создана и отобразится в таблице.

6. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение группы экземпляров VRRP

Вы можете изменить группу экземпляров VRRP в шаблоне CPE или на устройстве CPE. Группа экземпляров VRRP, измененная в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете изменить на устройстве CPE группу экземпляров VRRP, унаследованную из шаблона CPE.

Чтобы изменить группу экземпляров VRRP:

1. Перейдите к изменению группы экземпляров VRRP одним из следующих способов:

   - Если вы хотите изменить группу экземпляров VRRP в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRRP → Группы экземпляров VRRP**.

   - Если вы хотите изменить группу экземпляров VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **VRRP → Группы экземпляров VRRP** и установите флажок **Переопределить**.

   Отобразится таблица групп экземпляров VRRP.

2. Нажмите на кнопку **Изменить** рядом с группой экземпляров VRRP, которую вы хотите изменить.

3. В открывшемся окне при необходимости измените имя группы экземпляров VRRP и добавьте или удалите созданные экземпляры VRRP.

4. Нажмите на кнопку **Сохранить**.

   Группа экземпляров VRRP будет изменена и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление группы экземпляров VRRP

Вы можете удалить группу экземпляров VRRP в шаблоне CPE или на устройстве CPE. Группа экземпляров VRRP, удаленная в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете удалить на устройстве CPE группу экземпляров VRRP, унаследованную из шаблона CPE.

Удаленные группы экземпляров VRRP невозможно восстановить.

Чтобы удалить группу экземпляров VRRP:

1. Перейдите к удалению группы экземпляров VRRP одним из следующих способов:

   - Если вы хотите удалить группу экземпляров VRRP в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRRP → Группы экземпляров VRRP**.

   - Если вы хотите удалить группу экземпляров VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **VRRP → Группы экземпляров VRRP** и установите флажок **Переопределить**.

   Отобразится таблица групп экземпляров VRRP.

2. Нажмите на кнопку **Удалить** рядом с группой экземпляров VRRP, которую вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Группа экземпляров VRRP будет удалена и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Передача multicast-трафика с помощью протоколов PIM и IGMP

Kaspersky SD-WAN поддерживает передачу пакетов multicast-трафика между устройствами CPE и внешними сетевыми устройствами с помощью протоколов PIM и IGMP. Вы можете указать основные параметры работы протокола PIM на устройствах CPE, например используемые точки рандеву (англ. rendezvous points), после чего создать multicast-интерфейсы для взаимодействия с другими устройствами CPE. В качестве multicast-интерфейсов используются созданные сетевые интерфейсы.

Если между устройствами CPE устанавливается связность по протоколу PIM, и для них определены точки рандеву, multicast-интерфейсы могут получать по протоколу IGMP-запросы от клиентов. IGMP-запросы содержат IP-адреса источников, от которых клиенты хотят получать пакеты multicast-трафика. Когда источники отправляют пакеты multicast-трафика на точку рандеву, клиенты получают пакеты multicast-трафика.

При необходимости вы можете использовать протокол PIM для подключения устройств CPE ко внешним маршрутизаторам. Для этого вам нужно включить использование протокола PIM на mulitcast-интерфейсе, к которому подключен внешний маршрутизатор.

Настройка основных параметров PIM

Вы можете настроить основные параметры PIM в шаблоне CPE или на устройстве CPE. Основные параметры PIM, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

Чтобы настроить основные параметры PIM:

1. Перейдите к настройке основных параметров PIM одним из следующих способов:

   - Если вы хотите настроить основные параметры PIM в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Multicast**.

   - Если вы хотите настроить основные параметры PIM на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Multicast**.

   По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры PIM.

2. В раскрывающемся списке **Multicast** выберите **Включено**. Значение по умолчанию: **Выключено**.

3. Укажите точку рандеву для источников пакетов multicast-трафика и подключенных к устройству CPE клиентов:

   a. В блоке **RP IP** нажмите на кнопку **+ Добавить** и введите IPv4-адрес точки рандеву.

   b. Если вы хотите указать multicast-группу, связанную с точкой рандеву, в блоке **RP-группа** введите IPv4-префикс multicast-группы. Каждая точка рандеву может быть связана с отдельной multicast-группой.

   Точка рандеву будет указана и отобразится в блоках **RP IP** и **RP-группа**. Вы можете указать несколько точек рандеву и удалить точки рандеву. Для удаления точки рандеву нажмите рядом с ней на значок удаления ✕.

4. В поле **RP keepalive-таймер (сек.)** введите время жизни потоков трафика между источником и multicast-группой (S,G) в секундах. Отсчет времени начинается заново, если устройство CPE получает пакет register. Диапазон значений: от 31 до 60 000. Значение по умолчанию: `185`.

5. Если вы хотите фильтровать на устройстве CPE пакеты multicast-трафика с указанными IPv4-адресами источника, в раскрывающемся списке **Список допустимых регистраций PIM** выберите созданный список префиксов.

6. Если устройство CPE находится на последнем хопе, и вы хотите запретить на устройстве CPE переключение с общего дерева (англ. shared tree) на дерево кратчайшего пути (англ. Shortest Path Tree, SPT) при передаче пакетов multicast-трафика, выполните следующие действия:

   a. Установите флажок **Переключение SPT**. Этот флажок снят по умолчанию.

   b. Если вы хотите запретить или разрешить на устройстве CPE переключение с дерева точки рандеву (англ. Rendezvous Point Tree, RPT) на дерево кратчайшего пути при передаче пакетов трафика с указанными IPv4-префиксами источника от multicast-групп, в раскрывающемся списке **Список префиксов SPT** выберите созданный список префиксов. Запрет или разрешение на переключение определяется следующим образом:

      - Если список префиксов разрешает IPv4-префикс, переключение не происходит.

      - Если список префиксов запрещает IPv4-префикс, переключение происходит.

7. Если вы хотите выполнять ECMP-балансировку на устройстве CPE для распределения потоков multicast-трафика по нескольким маршрутам, выполните следующие действия:

   a. Установите флажок **ECMP**. Этот флажок снят по умолчанию. Для выполнения ECMP-балансировки требуется наличие нескольких маршрутов. Если ECMP-балансировка выключена, трафик передается по одному маршруту.

   b. Если вы хотите перераспределить весь трафик между оставшимися маршрутами при выходе из строя одного из multicast-интерфейсов, установите флажок **Перебалансировка ECMP**. Этот флажок снят по умолчанию, и при выходе из строя одного из multicast-интерфейсов перераспределяются только трафик, передававшийся через multicast-интерфейс.

8. В поле **Интервал присоединения/отказа PIM** введите интервал времени в секундах для отправки multicast-интерфейсами пакетов join/prune PIM-соседям. Диапазон значений: от 60 до 600. Значение по умолчанию: `60`.

9. В поле **PIM keepalive-таймер (сек.)** введите время жизни потоков трафика между источником и multicast-группой (S,G) в секундах. Отсчет времени начинается заново, если устройство CPE получает пакет join/prune. Диапазон значений: от 31 до 60 000. Значение по умолчанию: `210`.

10. Если вы хотите передавать на устройстве CPE пакеты трафика с указанными IPv4-префиксами источника от multicast-групп по запросу от клиента (англ. Source Specific Multicast, SSM), в раскрывающемся списке **Список префиксов SSM** выберите созданный список префиксов.

11. В раскрывающемся списке **Режим поиска RPF** выберите режим проверки Reverse Path Forwarding (RPF) на устройстве CPE:

    - **longer-prefix**.
    - **lower-distance**.
    - **mrib-only**.
    - **mrib-then-urib**. Это значение выбрано по умолчанию.
    - **urib-only**.

12. Если вы хотите добавить в таблицу multicast-маршрутизации устройства CPE статический IPv4-маршрут, выполните следующие действия:

    a. В блоке **Статические multicast-маршруты** нажмите на кнопку **+ Добавить**.

    b. В поле **IP назначения** введите IPv4-адрес назначения статического маршрута.

    c. В раскрывающемся списке **Тип** выберите тип источника статического маршрута:

    - **Адрес** – IPv4-адрес. При выборе этого значения в поле **Nexthop** введите IPv4-адрес источника статического маршрута.
    - **Интерфейс** – созданный сетевой интерфейс. При выборе этого значения в раскрывающемся списке **Nexthop** выберите сетевой интерфейс источника статического маршрута.

    d. При необходимости в поле **Дистанция** введите метрику статического маршрута. Диапазон значений: от 1 до 255.

    Статический маршрут будет добавлен и отобразится в блоке **Статические multicast-маршруты**. Вы можете добавить несколько статических маршрутов и удалить статические маршруты. Для удаления статического маршрута нажмите рядом с ним на значок удаления ✕.

13. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с multicast-интерфейсами

Вы можете посмотреть таблицу multicast-интерфейсов в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы multicast-интерфейсов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **Multicast → Интерфейсы**.
- Для просмотра таблицы multicast-интерфейсов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Multicast → Интерфейсы**.

Информация о multicast-интерфейсах отображается в следующих столбцах таблицы:

- **Сетевой интерфейс** – сетевой интерфейс, который используется как multicast-интерфейс.
- **PIM** – на multicast-интерфейсе включен обмен сообщениями по протоколу PIM с соседями:
    - **Включено**.
    - **Выключено**.
- **IGMP** – на multicast-интерфейсе включен обмен сообщениями по протоколу IGMP с соседями:
    - **Включено**.
    - **Выключено**.

- **Приоритет DR** – приоритет multicast-интерфейса. Multicast-интерфейс с наивысшим приоритетом становится выделенным маршрутизатором (англ. designated router) в LAN-сегменте. Чем выше введенное значение, тем выше приоритет multicast-интерфейса.

- **Унаследовано** – multicast-интерфейс унаследован из шаблона CPE:

  - **Да**.

  - **Нет**.

  Этот столбец отображается только на устройстве CPE.

- **Управление** – действия, которые можно выполнить с multicast-интерфейсом.

Создание multicast-интерфейса

Вы можете создать multicast-интерфейс в шаблоне CPE или на устройстве. Multicast-интерфейс, созданный в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать multicast-интерфейс:

1. Перейдите к созданию multicast-интерфейса одним из следующих способов:

   - Если вы хотите создать multicast-интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Multicast** → **Интерфейсы**.

   - Если вы хотите создать multicast-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Multicast** → **Интерфейсы** и установите флажок **Переопределить**.

   Отобразится таблица multicast-интерфейсов.

2. Нажмите на кнопку **+ Multicast-интерфейс**.

3. В открывшемся окне в раскрывающемся списке **Сетевой интерфейс** выберите созданный сетевой интерфейс, который вы хотите использовать как multicast-интерфейс.

4. Настройте протокол PIM на multicast-интерфейсе:

   a. В раскрывающемся списке **PIM** выберите **Включено**. Значение по умолчанию: **Выключено**.

   b. Если вы хотите перевести multicast-интерфейс в пассивный режим, установите флажок **Пассивный**. В пассивном режиме multicast-интерфейсы не обмениваются контрольными пакетами. Этот флажок снят по умолчанию.

   c. Если вы хотите запретить обмен bootstrap-пакетами на multicast-интерфейсе, снимите флажок **BSM**. Этот флажок установлен по умолчанию.

   d. Если вы хотите запретить обмен unicast bootstrap-пакетами на multicast-интерфейсе, снимите флажок **Unicast BSM**. Этот флажок установлен по умолчанию.

   e. В поле **Приоритет DR** введите приоритет multicast-интерфейса. Multicast-интерфейс с наивысшим приоритетом становится выделенным маршрутизатором (англ. designated router) в LAN-сегменте. Чем выше введенное значение, тем выше приоритет multicast-интерфейса. Диапазон значений: от 1 до 4 294 967 295. Значение по умолчанию: `1`.

   f. В поле **Hello (сек.)** введите интервал времени в секундах для отправки multicast-интерфейсом контрольных пакетов PIM-соседям. Диапазон значений: от 1 до 180. Значение по умолчанию: `30`.

   g. В поле **Hold (сек.)** введите интервал времени в секундах для получения multicast-интерфейсом контрольных пакетов от PIM-соседей. Если в течение указанного времени от PIM-соседа не поступает контрольных пакетов, multicast-интерфейс считает PIM-соседа недоступным. Диапазон значений: от 1 до 630. Значение по умолчанию: `105`.

   h. Если multicast-интерфейсу назначено несколько IP-адресов, и вы хотите использовать указанный IPv4-адрес источника при отправке PIM-сообщений, в поле **IP источника** введите IPv4-адрес.

5. Настройте протокол IGMP на multicast-интерфейсе:

   a. В раскрывающемся списке **IGMP** выберите **Включено**. Значение по умолчанию: **Выключено**.

   b. В раскрывающемся списке **Версия** выберите версию протокола IGMP на multicast-интерфейсе:

      - **2**.
      - **3**. Это значение выбрано по умолчанию.

   c. В поле **Интервал запроса (сек.)** введите интервал времени в секундах для отправки multicast-интерфейсом запросов (англ. queries) клиентам. Запросы используются, чтобы определить, требуется ли отправлять multicast-трафик клиентам. Диапазон значений: от 1 до 250. Значение по умолчанию: `125`.

   d. В поле **Время ответа на запрос (сек.)** введите время в секундах для получения multicast-интерфейсом ответов от клиентов. Если в течение указанного времени от клиента не поступает ответа на запрос, multicast-интерфейс не отправляет пакеты трафика. Диапазон значений: от 1 до 125. Значение по умолчанию: `10`.

   e. Если вы хотите указать multicast-группы, выполните следующие действия:

      1. В блоке **Группа присоединения** нажмите на кнопку **+ Добавить** и введите IPv4-адрес multicast-группы.
      2. Если вы хотите подключить multicast-интерфейс к указанному источнику multicast-группы, в блоке **Источник** введите IPv4-адрес источника.

      Multicast-группа будет указана и отобразится в блоках **Группа присоединения** и **Источник**. Вы можете указать несколько multicast-групп и удалить multicast-группы. Для удаления multicast-группы нажмите рядом с ней на значок удаления ✕.

      Вам нужно указать multicast-группы в одном из следующих случаев:

      - В сегменте сети есть постоянные клиенты, которым требуется быстро и стабильно отправлять пакеты трафика от multicast-группы.
      - В сегменте сети нет клиентов или узлы в сегменте не могут отправлять сообщения отчета (англ. report messages), но в сегмент требуется отправлять пакеты трафика от multicast-группы.

6. Нажмите на кнопку **Создать**.

   Multicast-интерфейс будет создан и отобразится в таблице.

7. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение multicast-интерфейса

Вы можете изменить параметры multicast-интерфейса в шаблоне CPE или на устройстве CPE. Multicast-интерфейс, измененный в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE.

Чтобы изменить multicast-интерфейс:

1. Перейдите к изменению multicast-интерфейса одним из следующих способов:

   - Если вы хотите изменить multicast-интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Multicast** → **Интерфейсы**.

   - Если вы хотите изменить multicast-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Multicast** → **Интерфейсы** и установите флажок **Переопределить**.

   Отобразится таблица multicast-интерфейсов.

2. Нажмите на кнопку **Изменить** рядом с multicast-интерфейсом, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры multicast-интерфейса. Описание параметров см. в инструкции по созданию multicast-интерфейса.

4. Нажмите на кнопку **Сохранить**.

   Multicast-интерфейс будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление multicast-интерфейса

Вы можете удалить multicast-интерфейс в шаблоне CPE или на устройстве CPE. Multicast-интерфейс, удаленный в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE.

Удаленные multicast-интерфейсы невозможно восстановить.

Чтобы удалить multicast-интерфейс:

1. Перейдите к удалению multicast-интерфейса одним из следующих способов:

   - Если вы хотите удалить multicast-интерфейс в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Multicast** → **Интерфейсы**.

   - Если вы хотите удалить multicast-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Multicast** → **Интерфейсы** и установите флажок **Переопределить**.

   Отобразится таблица multicast-интерфейсов.

2. Нажмите на кнопку **Удалить** рядом с multicast-интерфейсом, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Multicast-интерфейс будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Работа с виртуальными таблицами маршрутизации (VRF)

Kaspersky SD-WAN поддерживает технологию Virtual Routing and Forwarding (VRF) для создания виртуальных таблиц маршрутизации на устройствах CPE. Вы можете создать не более 100 виртуальных таблиц маршрутизации.

При создании виртуальной таблицы маршрутизации вам нужно выбрать сетевые интерфейсы, которые вы хотите в нее добавить. Один сетевой интерфейс невозможно добавить в несколько виртуальных таблиц маршрутизации. Сетевые интерфейсы для подключения устройства CPE к контроллеру и оркестратору автоматически добавляются в виртуальную таблицу маршрутизации по умолчанию, и вы не можете добавить их в другие виртуальные таблицы маршрутизации.

Если сетевые интерфейсы добавлены в разные виртуальные таблицы маршрутизации, подключенные к сетевым интерфейсам сети не имеют доступа друг к другу. При этом сетевым интерфейсам можно назначить IP-адреса из одинаковых или пересекающихся подсетей.

Когда вы создаете виртуальную таблицу маршрутизации, на устройстве CPE автоматически создается системный сетевой интерфейс, соответствующий этой виртуальной таблице маршрутизации. Системный сетевой интерфейс используется для передачи трафика между сетевыми интерфейсами в виртуальной таблице маршрутизации. Для работы системного сетевого интерфейса вам нужно создать для него запись в веб-интерфейсе оркестратора.

При создании виртуальной таблицы маршрутизации вы можете использовать функцию создания blackhole-маршрута для изоляции трафика. В этом случае на устройстве автоматически будет создан blackhole-маршрут 0.0.0.0/0, информация о котором отобразится в разделе **Статические маршруты**. Без использования blackhole-маршрута трафик может попадать в другие виртуальные таблицы маршрутизации.

Если сетевым интерфейсам в виртуальной таблице маршрутизации не назначены зоны межсетевого экрана, вам нужно убедиться, что по умолчанию межсетевой экран устройства CPE принимает пакеты трафика, пересылаемые между сетевыми интерфейсами и подсетями. Вы можете указать действия по умолчанию при настройке основных параметров межсетевого экрана.

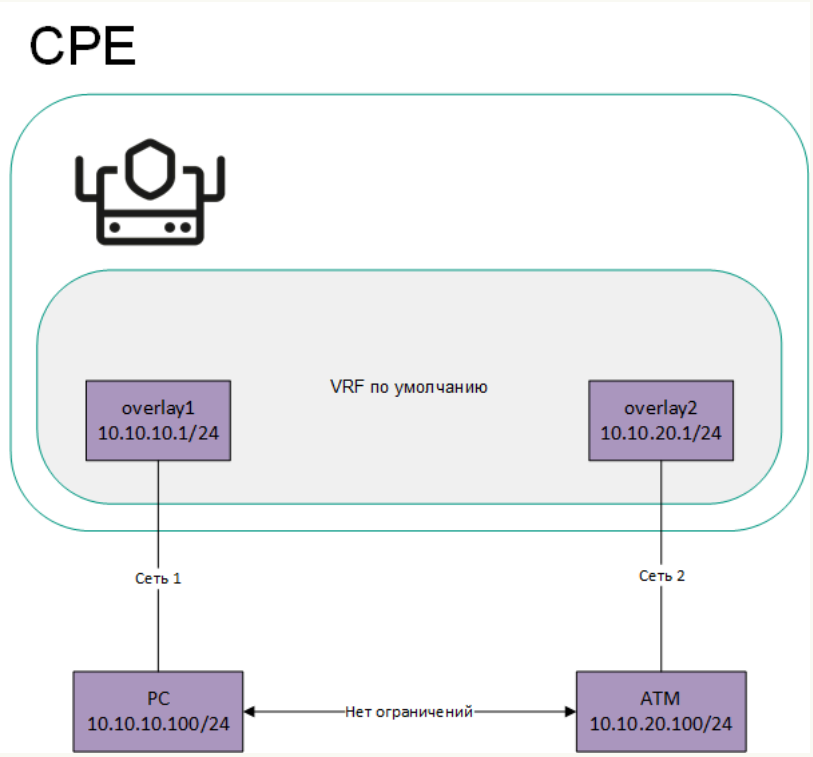
Если сетевым интерфейсам в виртуальной таблице маршрутизации назначены зоны межсетевого экрана и по умолчанию межсетевой экран устройства CPE не принимает пакеты трафика, пересылаемые между сетевыми интерфейсами и подсетями, вам нужно назначить системному сетевому интерфейсу зону межсетевого экрана. Назначенная зона межсетевого экрана также должна быть назначена одному из сетевых интерфейсов в виртуальной таблице маршрутизации.

Вы можете добавить в виртуальные таблицы маршрутизации BGP-маршруты и статические маршруты устройства CPE. Для добавления BGP-маршрутов в виртуальную таблицу маршрутизации вам нужно указать требуемую виртуальную таблицу маршрутизации при настройке основных параметров BGP. Для добавления статического маршрута в виртуальную таблицу маршрутизации вам нужно указать требуемую виртуальную таблицу маршрутизации при добавлении статического маршрута.

Виртуальные таблицы маршрутизации можно использовать в следующих сценариях:

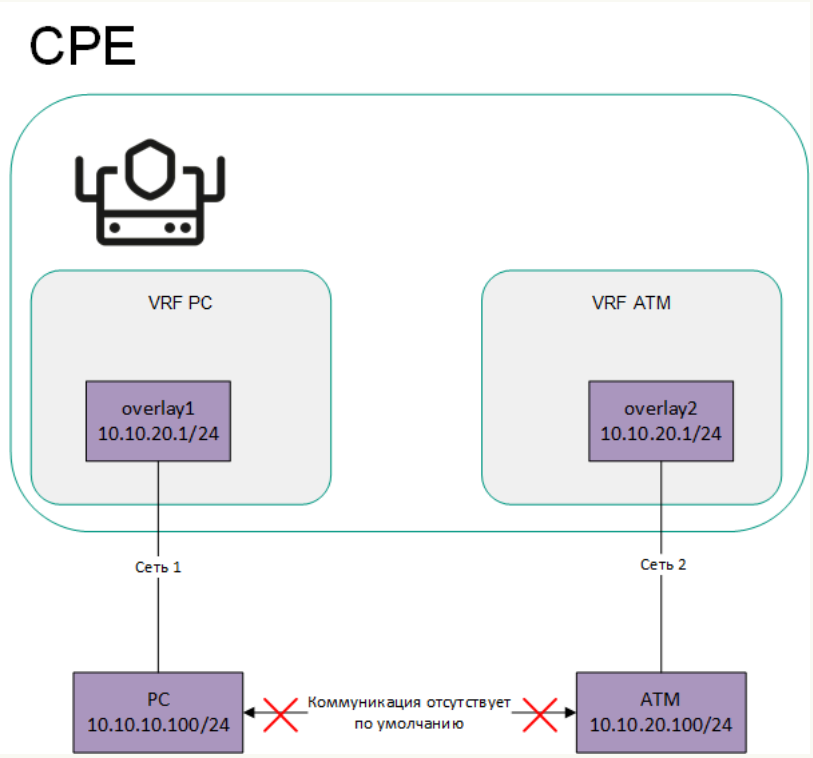
- **Сегментация сети с помощью виртуальных таблиц маршрутизации**.

Вы можете создать виртуальные таблицы маршрутизации, чтобы сегментировать сеть. На рисунке ниже сеть 1 построена между сетевым интерфейсом overlay1 и пользовательским персональными компьютерами PC, а сеть 2 – между сетевым интерфейсом overlay2 и банкоматами ATM. Оба сетевых интерфейса находятся в виртуальной таблице маршрутизации по умолчанию (VRF по умолчанию), поэтому сети имеют доступ друг к другу и являются небезопасными.



Подключенные к разным сетям сетевые интерфейсы в виртуальной таблице маршрутизации по умолчанию

Для изоляции сетей 1 и 2 сетевые интерфейсы overlay1 и overlay2 необходимо добавить в разные виртуальные таблицы маршрутизации VRF PC и VRF ATM, в результате чего будут созданы два сегмента (см. рисунок ниже).

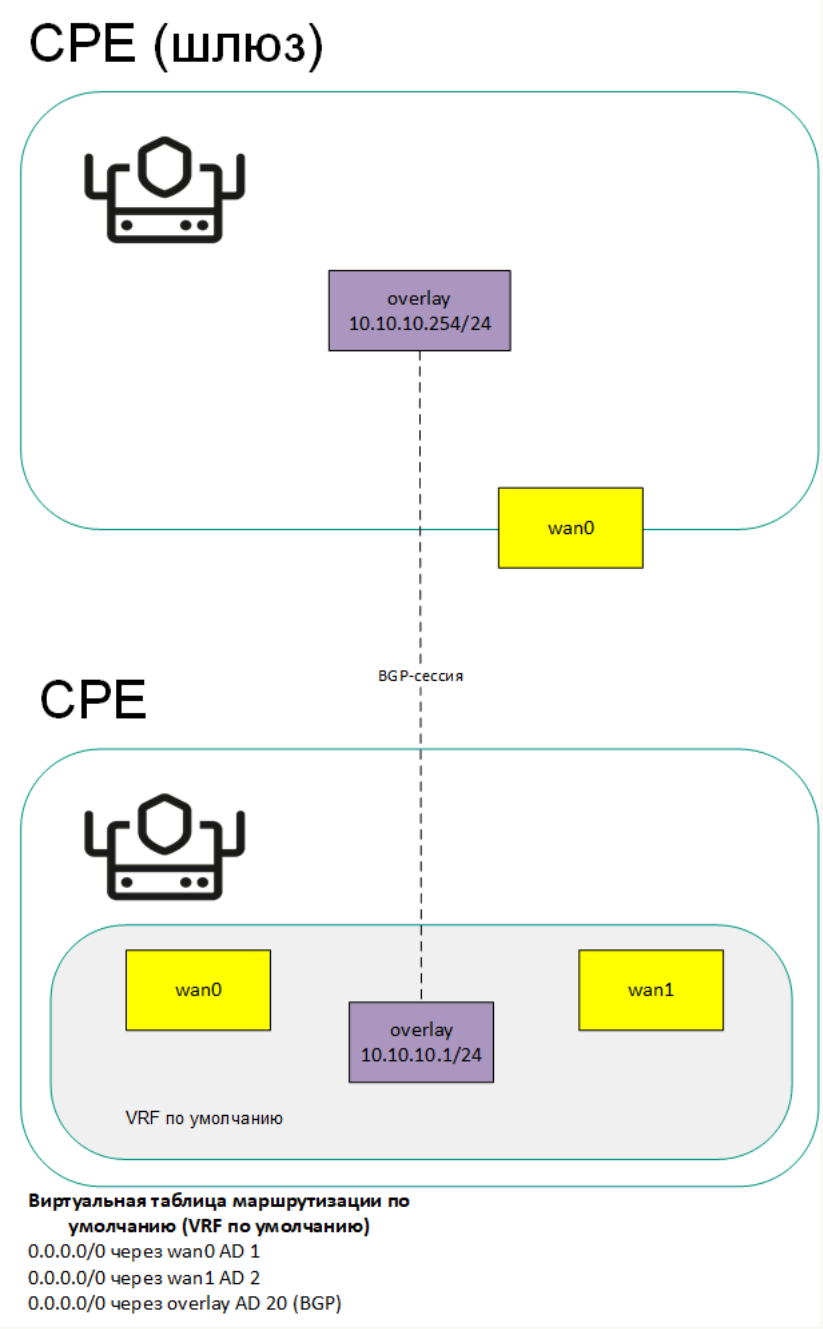


Подключенные к разным сетям сетевые интерфейсы в отдельных виртуальных таблицах маршрутизации

- Передача маршрута 0.0.0.0/0 по протоколу BGP.

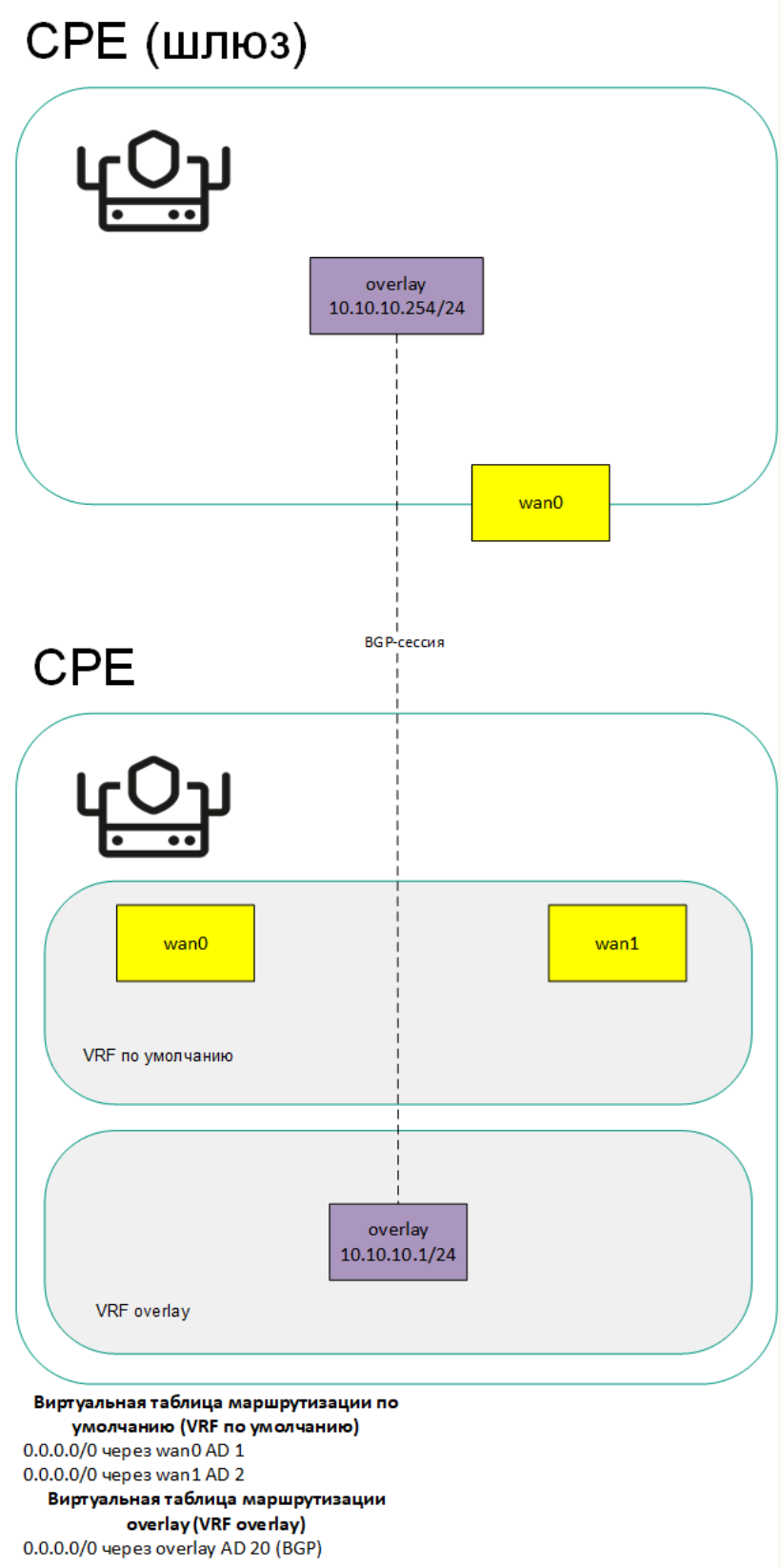
Вы можете создать отдельную виртуальную таблицу маршрутизации, чтобы передавать между устройствами маршрут 0.0.0.0/0 по протоколу BGP. На рисунке ниже представлено устройство CPE с ролью шлюза SD-WAN и стандартное устройство CPE. Все сетевые интерфейсы устройства CPE добавлены в виртуальную таблицу маршрутизации по умолчанию (VRF по умолчанию).

Если шлюз SD-WAN передает маршрут 0.0.0.0/0 по протоколу BGP с сетевого интерфейса overlay 10.10.10.254/24 на overlay 10.10.10.1/24, маршрут невозможно использовать. Это происходит потому, что в виртуальной таблице маршрутизации по умолчанию уже есть маршруты 0.0.0.0/0 с более низкой административной дистанцией для подключения к контроллеру и оркестратору.



Передача маршрута 0.0.0.0/0 на устройство CPE с виртуальной таблицей маршрутизации по умолчанию

Для передачи маршрута 0.0.0.0/0 по протоколу BGP через сетевой интерфейс overlay 10.10.10.254/24 на overlay 10.10.10.1/24 необходимо создать отдельную виртуальную таблицу маршрутизации VRF overlay для сетевого интерфейса overlay 10.10.10.1/24 и добавить в нее BGP-маршруты (см. рисунок ниже).



Передача маршрута 0.0.0.0/0 на устройство CPE с отдельной виртуальной таблицей маршрутизации для BGP-маршрутов

Вы можете посмотреть таблицу виртуальных таблиц маршрутизации в шаблоне CPE и на устройстве CPE:

- Для просмотра таблицы виртуальных таблиц маршрутизации в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **VRF**.
- Для просмотра таблицы виртуальных таблиц маршрутизации на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **CPE**, нажать на устройство CPE и выбрать вкладку **VRF**.

Информация о виртуальных таблицах маршрутизации отображается в следующих столбцах таблицы:

- **Имя** – имя виртуальной таблицы маршрутизации.
- **Унаследовано** – виртуальная таблица маршрутизации унаследована из шаблона CPE:
  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.
- **Таблица** – идентификатор виртуальной таблицы маршрутизации.
- **Интерфейсы** – сетевые интерфейсы, добавленные в виртуальную таблицу маршрутизации.

Настройка параметров ядра, связанных с виртуальными таблицами маршрутизации

Вы можете настроить параметры ядра, связанные с виртуальными таблицами маршрутизации, в шаблоне CPE или на устройстве CPE. Это необходимо для обеспечения правильной работы сетевых сервисов в созданных вами виртуальных таблицах маршрутизации. Параметры ядра, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

Чтобы настроить параметры ядра:

1. Перейдите к настройке параметров ядра одним из следующих способов:

   - Если вы хотите настроить параметры ядра в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRF** → **Основные параметры**.

   - Если вы хотите настроить параметры ядра на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **VRF** → **Основные параметры** и установите флажок **Переопределить**.

   Отобразятся параметры ядра.

2. При необходимости выполните одно из следующих действий:

   - Если вы хотите использовать сетевые сервисы UDP в виртуальных таблицах маршрутизации, установите флажок **Использовать сетевые сервисы UDP во всех VRF**. Этот флажок снят по умолчанию.

   - Если вы хотите использовать сетевые сервисы TCP в виртуальных таблицах маршрутизации, установите флажок **Использовать сетевые сервисы TCP во всех VRF**. Этот флажок снят по умолчанию.

   - Если вы не хотите использовать RAW-сокеты в виртуальных таблицах маршрутизации, снимите флажок **Использовать RAW-сокеты во всех VRF**. Этот флажок установлен по умолчанию.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Создание виртуальной таблицы маршрутизации

Вы можете создать виртуальную таблицу маршрутизации в шаблоне CPE или на устройстве CPE. Виртуальная таблица маршрутизации, созданная в шаблоне CPE, автоматически создается на всех устройствах CPE, которые используют шаблон CPE.

Чтобы создать виртуальную таблицу маршрутизации:

1. Перейдите к созданию виртуальной таблицы маршрутизации одним из следующих способов:

   - Если вы хотите создать виртуальную таблицу маршрутизации в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRF**.

   - Если вы хотите создать виртуальную таблицу маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE и выберите вкладку **VRF**.

   По умолчанию выбрана вкладка **VRF**, на которой отображается таблица виртуальных таблиц маршрутизации.

2. Нажмите на кнопку **+ VRF**.

3. В открывшемся окне в поле **Имя** введите имя виртуальной таблицы маршрутизации.

4. В поле **Таблица** введите идентификатор виртуальной таблицы маршрутизации. Диапазон значений: от 100 до 199.

5. Если хотите обеспечить дополнительную изоляцию трафика для виртуальной таблицы маршрутизации, установите флажок **Добавить blackhole-маршрут**. В результате при сохранении виртуальной таблицы маршрутизации в разделе **Статические маршруты** автоматически будет создан blackhole-маршрут 0.0.0.0/0.

   Если такой статический маршрут уже был создан ранее, при создании виртуальной таблицы маршрутизации флажок **Добавить blackhole-маршрут** будет установлен. При снятии флажка созданный ранее статический маршрут будет удален.

   По умолчанию флажок не установлен. При отсутствии blackhole-маршрута трафик может попадать в другие виртуальные таблицы маршрутизации.

6. В раскрывающемся списке **Интерфейсы** выберите созданный сетевой интерфейс, который вы хотите добавить в виртуальную таблицу маршрутизации. Вы не можете добавить один сетевой интерфейс в несколько виртуальных таблиц маршрутизации.

   Сетевой интерфейс будет добавлен и отобразится в нижней части окна. Вы можете добавить несколько сетевых интерфейсов и удалить сетевые интерфейсы. Для удаления сетевого интерфейса нажмите рядом с ним на кнопку **Удалить**.

   Если вы добавили в виртуальную таблицу маршрутизации сетевой интерфейс с именем в формате overlay.<номер>, например overlay.100, вам нужно установить флажки **Включать автоматически** и **Назначать IP, маршрут и шлюз** при создании или изменении сетевого интерфейса.

7. Нажмите на кнопку **Создать**.

   Виртуальная таблица маршрутизации будет создана и отобразится в таблице. На устройстве CPE будет создан системный сетевой интерфейс, соответствующий созданной виртуальной таблице маршрутизации. Если был установлен флажок **Добавить blackhole-маршрут**, в разделе **Статические маршруты** автоматически будет создан blackhole-маршрут 0.0.0.0/0.

8. Создайте запись в веб-интерфейсе оркестратора для системного сетевого интерфейса:

   a. Выберите вкладку **Сеть**.

      Отобразится таблица сетевых интерфейсов.

   b. Нажмите на кнопку **+ Сетевой интерфейс**.

   c. В открывшемся окне в поле **Псевдоним** введите имя виртуальной таблицы маршрутизации, которое вы указали на шаге 3 этой инструкции. Максимальная длина имени – 15 символов.

   d. Если сетевым интерфейсам в виртуальной таблице маршрутизации назначены зоны межсетевого экрана, и по умолчанию межсетевой экран устройства CPE не принимает пакеты трафика, пересылаемые между сетевыми интерфейсами и подсетями, в раскрывающемся списке **Зона** выберите зону межсетевого экрана. Выбранная зона межсетевого экрана также должна быть назначена одному из сетевых интерфейсов в виртуальной таблице маршрутизации.

   e. В поле **Имя интерфейса** введите имя виртуальной таблицы маршрутизации, которое вы указали на шаге 3 этой инструкции. Максимальная длина имени – 256 символов.

9. Нажмите на кнопку **Создать**.

   Запись для системного сетевого интерфейса будет создана и отобразится в таблице.

10. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Изменение виртуальной таблицы маршрутизации

Вы можете изменить виртуальную таблицу маршрутизации в шаблоне CPE или на устройстве. Виртуальная таблица маршрутизации, измененная в шаблоне CPE, автоматически изменяется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете изменить на устройстве CPE виртуальную таблицу маршрутизации, унаследованную из шаблона CPE.

Чтобы изменить виртуальную таблицу маршрутизации:

1. Перейдите к изменению виртуальной таблицы маршрутизации одним из следующих способов:

   - Если вы хотите изменить виртуальную таблицу маршрутизации в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRF**.

   - Если вы хотите изменить виртуальную таблицу маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE и выберите вкладку **VRF**.

   По умолчанию выбрана вкладка **VRF**, на которой отображается таблица виртуальных таблиц маршрутизации.

2. Нажмите на кнопку **Изменить** рядом с виртуальной таблицей маршрутизации, которую вы хотите изменить.

3. В открывшемся окне измените необходимые параметры виртуальной таблицы маршрутизации.

4. Нажмите на кнопку **Сохранить**.

   Виртуальная таблица маршрутизации будет изменена и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Удаление виртуальной таблицы маршрутизации

Вы можете удалить виртуальную таблицу маршрутизации в шаблоне CPE или на устройстве CPE. Виртуальная таблица маршрутизации, удаленная в шаблоне CPE, автоматически удаляется на всех устройствах CPE, которые используют шаблон CPE. Вы не можете удалить на устройстве CPE виртуальную таблицу маршрутизации, унаследованную из шаблона CPE.

Удаленные виртуальные таблицы маршрутизации невозможно восстановить.

Чтобы удалить виртуальную таблицу маршрутизации:

1. Перейдите к удалению виртуальной таблицы маршрутизации одним из следующих способов:

   - Если вы хотите удалить виртуальную таблицу маршрутизации в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **VRF**.

   - Если вы хотите удалить виртуальную таблицу маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **VRF**.

   По умолчанию выбрана вкладка **VRF**, на которой отображается таблица виртуальных таблиц маршрутизации.

2. Нажмите на кнопку **Удалить** рядом с виртуальной таблицей маршрутизации, которую вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Виртуальная таблица маршрутизации будет удалена и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Отслеживание информации о пакетах трафика с помощью протокола NetFlow

Kaspersky SD-WAN поддерживает протокол NetFlow версии 1, 5 и 9 для отслеживания информации о пакетах трафика на устройстве CPE.

Для централизованной настройки протокола NetFlow на устройствах CPE используются шаблоны NetFlow. Вам нужно указать основные параметры в шаблоне NetFlow, после чего указать шаблон NetFlow при добавлении или ручной регистрации устройств CPE, чтобы не настраивать каждое отдельное устройство CPE. Если вы измените параметр в шаблоне NetFlow, параметр автоматически изменится на всех устройствах CPE, которые используют шаблон NetFlow. Если вы измените параметр на устройстве CPE, параметр перестанет зависеть от шаблона NetFlow и при изменении в шаблоне NetFlow не будет изменяться на устройстве CPE.

При настройке основных параметров NetFlow вы можете указать до четырех NetFlow-коллекторов. Для отправки устройством CPE информации о пакетах трафика NetFlow-коллекторам вам нужно включить протокол NetFlow на сетевых интерфейсах. Протокол NetFlow можно включить при создании или изменении сетевого интерфейса.

Работа с шаблонами NetFlow

Для просмотра таблицы шаблонов NetFlow вам нужно в меню перейти в раздел **SD-WAN → Шаблоны NetFlow**. По умолчанию на портале администратора создан шаблон NetFlow **Default NetFlow template**, на основании которого создаются все остальные шаблоны NetFlow. Информация о шаблонах NetFlow отображается в следующих столбцах таблицы:

- **ID** – идентификатор шаблона NetFlow.
- **Имя** – имя шаблона NetFlow.
- **Использование** – использование шаблона NetFlow устройствами CPE:
  - **Да**.
  - **Нет**.
- **Изменено** – дата и время последнего изменения параметров шаблона CPE.
- **Пользователь** – имя пользователя, который создал шаблон NetFlow.
- **Владелец** – тенант, к которому относится шаблон NetFlow.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Вы можете выбрать назначенный шаблон NetFlow, чтобы он был предварительно выбран при добавлении и ручной регистрации устройства CPE. Тенантам нужно вручную создать и выбрать назначенный шаблон NetFlow на портале самообслуживания.

Создание шаблона NetFlow

Чтобы создать шаблон NetFlow:

1. В меню перейдите в раздел **SD-WAN → Шаблоны NetFlow**.

   Отобразится таблица шаблонов NetFlow.

2. В верхней части страницы нажмите на кнопку **+ Шаблон NetFlow**.
3. В открывшемся окне введите имя шаблона NetFlow.
4. Нажмите на кнопку **Создать**.

   Шаблон NetFlow будет создан и отобразится в таблице.

Вам нужно настроить созданный шаблон NetFlow. Более подробно о параметрах шаблона NetFlow см. в инструкции по настройке основных параметров NetFlow.

Выбор назначенного шаблона NetFlow

Вы можете выбрать назначенный шаблон NetFlow, чтобы он был предварительно выбран при добавлении и ручной регистрации устройства CPE. Тенантам нужно вручную создать и выбрать назначенный шаблон NetFlow на портале самообслуживания.

Чтобы выбрать назначенный шаблон NetFlow:

1. В меню перейдите в раздел **SD-WAN → Шаблоны NetFlow**.

   Отобразится таблица шаблонов NetFlow.

2. Нажмите на шаблон NetFlow, который вы хотите сделать назначенным шаблоном NetFlow.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Установить назначенным**.

Шаблон NetFlow станет назначенным шаблоном NetFlow.

Импорт шаблона NetFlow

Вы можете экспортировать шаблон NetFlow, после чего импортировать его в другой шаблон NetFlow. Параметры шаблона NetFlow выстраиваются в соответствии с параметрами импортированного шаблона NetFlow. При импорте можно выбрать параметры, которые вы хотите оставить без изменений. Шаблон NetFlow, в который был импортирован другой шаблон NetFlow, остается примененным к устройствам CPE, но параметры устройств CPE не изменяются.

Чтобы импортировать шаблон NetFlow:

1. В меню перейдите в раздел **SD-WAN → Шаблоны NetFlow**.

   Отобразится таблица шаблонов NetFlow.

2. Нажмите на шаблон NetFlow, который вы хотите экспортировать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Экспортировать**.

   На ваше локальное устройство сохранится архив в формате TAR.GZ. В архиве не содержится информация об устройствах CPE, использующих шаблон NetFlow.

4. Нажмите на шаблон NetFlow, в который вы хотите импортировать шаблон NetFlow.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

5. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Импортировать**.

6. В открывшемся окне снимите флажки рядом с параметрами шаблона NetFlow, которые вы хотите оставить без изменения после импорта.

7. В поле **Файл** укажите путь к архиву в формате TAR.GZ.

8. Нажмите на кнопку **Импортировать**.

Параметры шаблона NetFlow будут изменены в соответствии с параметрами импортированного шаблона NetFlow.

Клонирование шаблона NetFlow

Вы можете клонировать шаблон NetFlow, чтобы создать такой же шаблон NetFlow с другим именем.

Чтобы клонировать шаблон NetFlow:

1. В меню перейдите в раздел **SD-WAN → Шаблоны NetFlow**.

   Отобразится таблица шаблонов NetFlow.

2. Нажмите на шаблон NetFlow, который вы хотите клонировать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Клонировать**.

4. В открывшемся окне введите имя нового шаблона NetFlow.

5. Нажмите на кнопку **Клонировать**.

Клон шаблона NetFlow с новым именем будет создан и отобразится в таблице.

Просмотр использования шаблона NetFlow

При необходимости вы можете посмотреть, какие устройства CPE используют шаблон NetFlow. Например, если шаблон NetFlow используется, его невозможно удалить.

Чтобы посмотреть, используется ли шаблон NetFlow:

1. В меню перейдите в раздел **SD-WAN → Шаблоны NetFlow**.

   Отобразится таблица шаблонов NetFlow.

2. Нажмите на шаблон NetFlow, использование которого вы хотите посмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Показать использование**.

Откроется окно с таблицей устройств CPE, использующих шаблон NetFlow.

Удаление шаблона NetFlow

Вы не можете удалить шаблон NetFlow, если он используется хотя бы одним устройством CPE. Для удаления шаблона NetFlow, который используется устройствами CPE, вам нужно сначала изменить шаблон NetFlow устройств CPE. Вы можете посмотреть, какие устройства CPE используют шаблон NetFlow.

Удаленные шаблоны NetFlow невозможно восстановить.

Чтобы удалить шаблон NetFlow:

1. В меню перейдите в раздел **SD-WAN** → **Шаблоны NetFlow**.

   Отобразится таблица шаблонов NetFlow.

2. Нажмите на шаблон NetFlow, который вы хотите удалить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Шаблон NetFlow будет удален и перестанет отображаться в таблице.

Настройка основных параметров NetFlow

Вы можете настроить основные параметры NetFlow в шаблоне NetFlow или на устройстве CPE. Основные параметры NetFlow, указанные в шаблоне NetFlow, автоматически распространяются на все устройства CPE, которые используют шаблон NetFlow.

Чтобы настроить основные параметры NetFlow:

1. Перейдите к настройке основных параметров NetFlow одним из следующих способов:

   - Если вы хотите настроить основные параметры NetFlow в шаблоне NetFlow, в меню перейдите в раздел **SD-WAN** → **Шаблоны NetFlow** и нажмите на шаблон NetFlow.

   - Если вы хотите настроить основные параметры NetFlow на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **NetFlow** и установите флажок **Переопределить**.

   Отобразятся основные параметры NetFlow.

2. В раскрывающемся списке **NetFlow** выберите **Включено**. Значение по умолчанию: **Выключено**.

3. Укажите NetFlow-коллектор:

   a. В блоке **Коллекторы** нажмите на кнопку **+ Добавить**.

   b. В блоке **Хост** введите IPv4-адрес NetFlow-коллектора.

   c. В блоке **Порт** введите номер порта NetFlow-коллектора. Диапазон значений: от 1 до 65 535.

   NetFlow-коллектор будет указан и отобразится в блоке **Коллекторы**. Вы можете указать не более четырех NetFlow-коллекторов и удалить NetFlow-коллектор. Для удаления NetFlow-коллектора нажмите рядом с ним на значок удаления ✕.

4. В раскрывающемся списке **Версия экспорта** выберите версию протокола NetFlow:

   - **1**.
   - **5**.
   - **9**. Это значение выбрано по умолчанию.

5. В раскрывающемся списке **Уровень отслеживания** выберите, какую информацию о пакетах трафика отслеживает устройство CPE:

   - **ETHER** – отслеживать следующую информацию:
     - IP-адрес и порт источника и назначения;
     - MAC-адрес источника и назначения;
     - внешняя метка VLAN;
     - используемый протокол.
   - **FULL** – отслеживать IP-адрес и порт источника и назначения, а также используемый протокол. Это значение выбрано по умолчанию.
   - **VLAN** – отслеживать следующую информацию:
     - IP-адрес и порт источника и назначения;
     - внешняя метка VLAN;
     - используемый протокол.
   - **PROTO** – отслеживать IP-адрес источника и назначения, а также используемый протокол.
   - **IP** – отслеживать IP-адрес источника и назначения.

6. В поле **Максимум потоков** введите максимальное количество потоков трафика, которое устройство CPE может одновременно отслеживать. Диапазон значений: от 1 до 65 535. Значение по умолчанию: `8192`.

   Чем выше введенное значение, тем выше нагрузка на процессор устройства CPE.

7. В поле **Частота выборки** введите, как часто устройство CPE отслеживает информацию о пакетах трафика. Например, если вы вводите `10`, устройство CPE отслеживает информацию о каждом десятом пакете трафика. Диапазон значений: от 1 до 8192. Значение по умолчанию: `1024`.

   Чем меньше введенное значение, тем выше точность информации и нагрузка на процессор устройства CPE.

8. В поле **Время жизни (сек.)** введите максимальное время в секундах, в течение которого устройство CPE может отслеживать информацию о потоке трафика. Для выключения этой функции введите `0`. Диапазон значений: от 1 до 9999. Значение по умолчанию: `60`.

9. В поле **Лимит хопов** введите максимальное количество хопов до NetFlow-коллекторов. Диапазон значений: от 1 до 255. Значение по умолчанию: `64`.

10. Если вы хотите, чтобы устройство CPE отслеживало IPv6-трафик, в раскрывающемся списке **Отслеживать IPv6** выберите **Включено**. Значение по умолчанию: **Выключено**.

11. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона NetFlow или устройства CPE.

Для отправки устройством CPE информации о пакетах трафика NetFlow-коллекторам вам нужно включить протокол NetFlow на сетевых интерфейсах. Протокол NetFlow можно включить при создании или изменении сетевого интерфейса.

Изменение шаблона NetFlow устройства CPE

Чтобы изменить шаблон NetFlow устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, шаблон NetFlow которого вы хотите изменить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В раскрывающемся списке **Шаблон NetFlow** выберите созданный шаблон NetFlow.

4. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Диагностика устройства CPE

Вы можете запросить диагностическую информацию устройства CPE, например информацию об использовании протоколов BGP, OSPF и PIM. Результаты запроса диагностической информации отображаются в веб-интерфейсе оркестратора, и при необходимости их можно скачать в виде файла в формате TXT.

Kaspersky SD-WAN также поддерживает следующие утилиты для диагностики устройства CPE:

- Ping – утилита для тестирования соединения между устройством CPE и указанным IPv4-адресом.
- Traceroute – утилита для определения маршрута между устройством CPE и указанным IPv4-адресом.
- Tcpdump – утилита для захвата трафика на устройстве CPE. При захвате с трафика снимается копия и трафик продолжает передаваться до назначения.
- Iperf – утилита для диагностики производительности сети. Вы можете использовать устройство CPE как iperf-сервер или как iperf-клиент.
- Sweep – утилита для выполнения следующих действий на устройстве CPE:
  - очистка ARP-кеша;
  - перезапуск процесса FRR (Free Range Routing);
  - очистка таблицы NAT-сессий;
  - перезапуск модемов.
- OpenFlow dump – утилита для запроса dump-flows и dump-groups, сгенерированных виртуальным коммутатором устройства CPE.

В результате работы утилит tcpdump, iperf и OpenFlow dump генерируются отчеты, которые вы можете скачать и удалить.

Запуск утилиты – это задача, которую устройство CPE получает от оркестратора, и ее выполнение происходит в соответствии с интервалом времени для отправки устройством CPE REST API-запросов оркестратору. Если вы хотите, чтобы утилиты запускались быстрее, вы можете включить интерактивный режим на устройстве CPE.

В *интерактивном режиме* устройство CPE имеет более короткий интервал времени для отправки REST API-запросов оркестратору. Интерактивный режим выключается автоматически по прошествии указанного вами времени. Вы можете указать следующие параметры, связанные с интерактивным режимом, при настройке подключения устройства CPE к оркестратору и контроллеру:

- интервал времени для отправки устройством CPE REST API-запросов оркестратору в интерактивном режиме;
- время, по прошествии которого интерактивный режим автоматически выключается.

Запрос диагностической информации

Чтобы запросить диагностическую информацию:

1. В меню перейдите в раздел **SD-WAN** → **CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запросить диагностическую информацию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Диагностическая информация**.

   Отобразятся параметры запроса диагностической информации.

4. Нажмите на кнопку **Запросить диагностическую информацию**.

   Дождитесь получения диагностической информации с устройства CPE.

5. В раскрывающемся списке **Имя** выберите тип диагностической информации, которую вы хотите отобразить:

   - **disk usage** – информация об использовании диска устройства CPE. Это значение выбрано по умолчанию.
   - **ip addresses** – информация об IP-адресах, назначенных физическим портам или виртуальным интерфейсам операционной системы устройства CPE.
   - **vrf data** – информация о виртуальных таблицах маршрутизации.
   - **ip neighbors** – информация об IP-соседях устройства CPE, полученных из ARP-таблицы или с помощью протокола обнаружения соседей (англ. Neighbor Discovery Protocol).
   - **ip routes** – информация о маршрутах IPv4 и IPv6.
   - **ip rules** – информация о правилах маршрутизации.
   - **iptables** – информация об iptables.
   - **cpe log** – локальный журнал устройства CPE.
   - **ovs-ofctl show** – информация о виртуальном коммутаторе.
   - **ovs-vsctl show** – информация о соединении между виртуальным коммутатором и контроллерами.
   - **ovs-vsctl list controller** – информация о контроллерах, указанных для виртуального коммутатора.
   - **show ip ospf** – информация о процессе OSPF-маршрутизации.
   - **show ip ospf interface** – информация об OSPF-интерфейсах.
   - **show ip ospf neighbor** – информация об OSPF-соседях.
   - **show ip ospf database** – база данных OSPF.
   - **bgp show ip route** – информация о BGP-маршрутах.
   - **show ip bgp** – информация о процессе BGP-маршрутизации.
   - **show ip bgp summary** – краткая информация о процессе BGP-маршрутизации.
   - **top process** – информация о Linux-процессах.
   - **uptime** – время работы устройства CPE.
   - **time sync** – информация о синхронизации времени на устройстве CPE с помощью NTP-сервера.
   - **netstat** – информация о сетевых соединениях, которые установило устройство CPE.
   - **sdwan interfaces** – информация об интерфейсах SD-WAN.
   - **modems** – информация о модемах.

     После получения с устройства информация отображается также в разделе **Модемы** в области настройки параметров устройства CPE (**SD-WAN** → **CPE**).

- **show bfd peers** –информация о BFD-соседях.
- **netflow dump-flows** – информация о NetFlow-потоках.
- **netflow statistics** – информация об использовании протокола NetFlow.
- **show bfd peers brief** – краткая информация о BFD-соседях.
- **show ip pim bsr** – информация о текущем bootstrap-маршрутизаторе (англ. bootstrap router, BSR).
- **show ip pim bsrp-info** – информация о связке group-to-rp mapping, полученной от boostrap-маршрутизатора.
- **show ip pim interface** – информация о PIM-интерфейсах. Вы можете настроить протокол PIM при создании и изменении mutlicast-интерфейса.
- **show ip pim interface traffic** – информация о PIM-трафике.
- **show ip pim join** – информация о multicast-группах, к которым подключено устройство CPE.
- **show ip pim neighbor** – информация о PIM-соседях.
- **show ip pim nexthop** – информация о следующих хопах multicast-групп.
- **show ip pim rp-info** – информация о точках рандеву. Вы можете указать точки рандеву при настройке основных параметров PIM.
- **show ip pim secondary** – информация о резервном PIM-маршрутизаторе.
- **show ip pim state** – информация о состоянии протокола PIM.
- **show ip pim statistics** – информация об использовании протокола PIM.
- **show ip pim upstream** – информация о PIM-источниках.
- **show ip igmp groups** – информация об IGMP-группах.
- **show ip igmp interface** – информация об IGMP-интерфейсах. Вы можете настроить протокол IGMP при создании и изменении mutlicast-интерфейса.
- **show ip igmp interface detail** – подробная информация об IGMP-интерфейсах.
- **show ip igmp sources** – информация об IGMP-источниках.
- **igmp statistics** – информация об использовании протокола IGMP.
- **show ip multicast** – информация о процессе multicast-маршрутизации.
- **show ip mroute** – информация о multicast-маршрутах.
- **show ip mroute summary** – краткая информация о multicast-маршрутах.
- **vswitchd log** – журнал процесса ovs-vswitchd.
- **firewall config** – информация о межсетевом экране.

- **sw version** – версия прошивки устройства CPE.
- **vrrp stats** – краткая информация об использовании протокола VRRP.
- **vrrp data** – информация об использовании протокола VRRP.

6. Если вы хотите отфильтровать отображаемую диагностическую информацию, выполните следующие действия:

   a. В поле **Найти строку по паттерну** введите слова, которые должны содержаться в строках диагностической информации, чтобы эти строки были отображены. Максимальная длина: 64 символа. Если вы хотите, чтобы отобразились только строки без введенных слов, установите флажок **Показать все, за исключением найденного**. Этот флажок снят по умолчанию.

   b. В поле **Показать линии до и после** введите количество пустых строк, которые вы хотите отобразить до и после каждой строки диагностической информации.

7. Если вы хотите скачать файл с диагностической информацией, нажмите на кнопку **Скачать**.

   На ваше локальное устройство сохранится файл в формате TXT.

Использование режима отладки для протоколов динамической маршрутизации на устройствах CPE

С помощью режима отладки вы можете выполнять детальную диагностику протоколов BGP и OSPF на устройствах CPE. При включении режима отладки на устройстве CPE для журналов процесса FRR устанавливается уровень детализации **Отладка**, и на устройстве выполняются соответствующие команды **debug <...>** из пакета FRR.

Включение режима отладки на CPE может существенно увеличить нагрузку на процессор. Рекомендуется выполнять эту процедуру в нерабочее время, чтобы избежать проблем с производительностью. Если устройство CPE стало недоступным после включения режима отладки, отключите режим отладки в оркестраторе и перезагрузите CPE.

Чтобы включить режим отладки:

1. В меню перейдите в раздел **SD-WAN → CPE**.

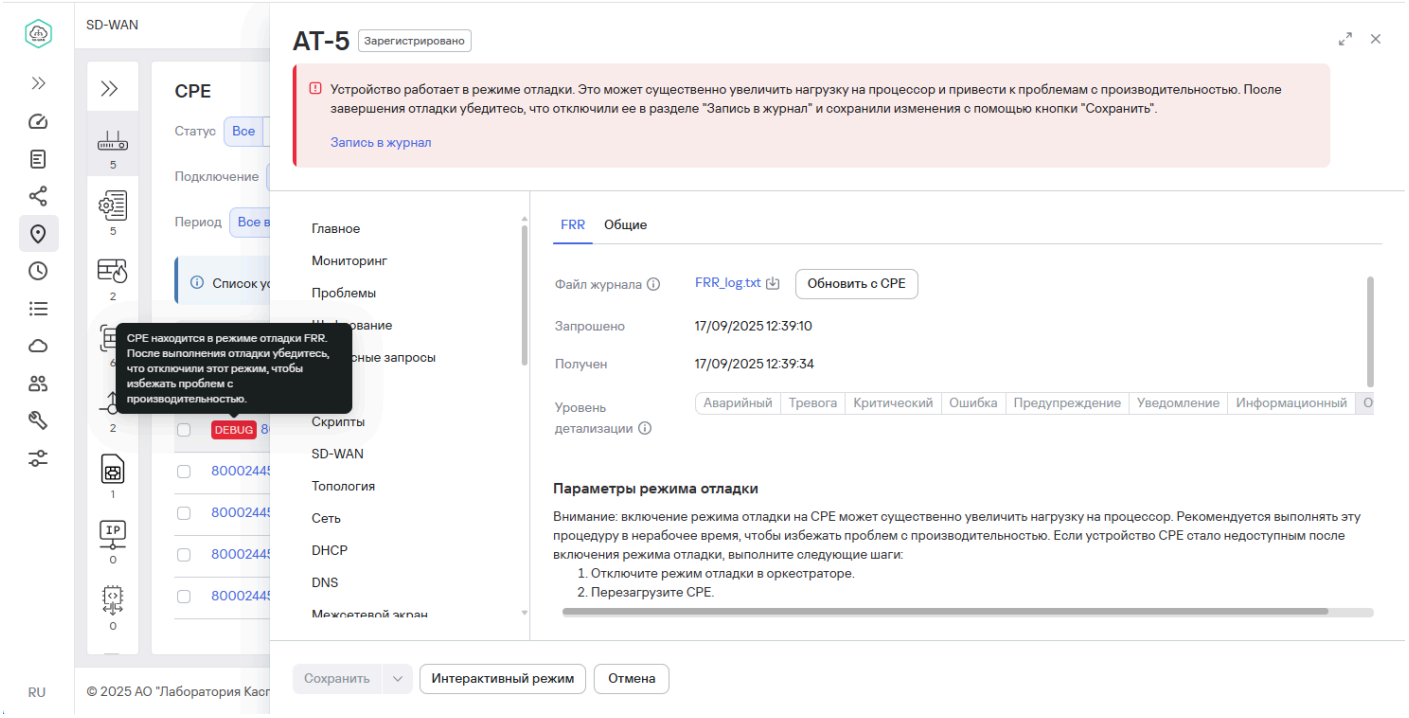
   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите включить режим отладки.
3. Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.
4. В меню слева выберите раздел **Журналы** и перейдите на вкладку **FRR**.
5. Включите переключатель **Режим отладки**.

6. На появившихся вкладках **BGP** и **OSPF** укажите необходимые параметры для команд отладки FRR. Для включения режима отладки вам необходимо указать хотя бы один параметр на любой из вкладок.

7. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE немедленно, или запланируйте отложенное сохранение, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Устройство CPE, на котором включен режим отладки, отображается в таблице в разделе **SD-WAN → CPE** со значком DEBUG рядом с его DPID.



Устройство CPE находится в режиме отладки

Чтобы скачать файл журнала отладки, запросите его с устройства, нажав на кнопку **Запросить с CPE** или **Обновить с CPE**, если файл уже был запрошен ранее, и, дождавшись загрузки файла в оркестратор, нажмите на ссылку для скачивания. Содержимое файла перезаписывается при каждом новом запросе. Учтите, что объем памяти для хранения файла ограничен, и по достижению лимита в файл не попадут новые записи.

Указание NTP-серверов на устройствах CPE

Вам нужно указать внутренний или внешний NTP-сервер, либо пул серверов для устройств CPE, чтобы на устройствах CPE отображалось точное время. Устройство CPE можно использовать как NTP-сервер, чтобы отображать точное время на сетевых устройствах, которые подключены к устройству CPE.

Вы можете указать NTP-сервер в шаблоне CPE или на устройстве CPE. NTP-серверы, указанные в шаблоне CPE, автоматически указываются на всех устройствах CPE, которые используют шаблон CPE.

Чтобы указать NTP-сервер на устройствах CPE:

1. Перейдите к указанию NTP-сервера одним из следующих способов:

   - Если вы хотите указать NTP-сервер в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **NTP**.

   - Если вы хотите указать NTP-сервер на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **NTP** и установите флажок **Переопределить**.

   Отобразятся параметры подключения к NTP-серверу.

2. Если вы хотите не указывать NTP-сервер для устройства CPE, снимите флажок **Подключиться к NTP-серверу**. Этот флажок установлен по умолчанию.

3. Если вы хотите использовать устройство CPE как NTP-сервер, установите флажок **Использовать как NTP-сервер**. Этот флажок снят по умолчанию.

4. Укажите NTP-сервер или пул серверов:

   a. В блоке **NTP-серверы** нажмите на кнопку **+ Добавить**.

   b. В отобразившемся поле введите IP-адрес или FQDN NTP-сервера, либо пула серверов. Поддерживаются следующие форматы IP-адреса и FQDN:

      - Для указания NTP-сервера введите IP-адрес или FQDN в формате `server <IP-адрес или FQDN>`, например `server 0.pool.ntp.org`.

      - Для указания пула NTP-серверов введите IP-адрес или FQDN в формате `pool <IP-адрес или FQDN>`, например `pool pool.ntp.org`.

   NTP-сервер будет указан и отобразится в блоке **NTP-серверы**. Вы можете указать несколько NTP-серверов и удалить NTP-серверы. Для удаления NTP-сервера нажмите рядом с ним на значок удаления ✕.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Вы можете запросить диагностическую информацию, чтобы посмотреть параметры синхронизации времени на устройстве CPE.

Включение интерактивного режима

Вы можете указать следующие параметры, связанные с интерактивным режимом, при настройке подключения устройства CPE к оркестратору и контроллеру:

- интервал времени для отправки устройством CPE REST API-запросов оркестратору в интерактивном режиме;

- время, по прошествии которого интерактивный режим автоматически выключается.

Чтобы включить интерактивный режим:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите включить интерактивный режим.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки нажмите на кнопку **Интерактивный режим**.

Интерактивный режим будет включен на устройстве CPE.

Запуск утилиты ping

Чтобы запустить утилиту ping:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту ping.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты**.

   По умолчанию выбрана вкладка **Ping**, на которой отображаются параметры утилиты ping.

4. В поле **IP-адрес назначения** введите IPv4-адрес, на который устройство CPE отправляет ICMP-запросы.

5. Если вы хотите, чтобы устройство CPE отправило ICMP-запросы с созданного сетевого интерфейса, в раскрывающемся списке **Сетевой интерфейс источника** выберите сетевой интерфейс.

6. В поле **Количество** введите количество ICMP-запросов, которое отправляет устройство CPE. Диапазон значений: от 1 до 1 000 000. Значение по умолчанию: `5`.

7. В поле **Время (сек.)** введите время в секундах, по прошествии которого устройство CPE должно получить ICMP-ответ, чтобы считать запрос успешным. Диапазон значений: от 1 до 3600. Значение по умолчанию: `2`.

8. В поле **Размер** введите размер ICMP-запроса в байтах. Диапазон значений: от 1 до 65 535. Значение по умолчанию: `56`

9. В поле **TTL** введите максимальное количество хопов для ICMP-запросов. Диапазон значений: от 1 до 255. Значение по умолчанию: `255`.

10. В поле **Интервал** введите интервал времени в секундах для отправки устройством CPE ICMP-запросов на указанный IPv4-адрес. Диапазон значений: от 1 до 300. Значение по умолчанию: `1`.

11. Нажмите на кнопку **Запустить**.

Утилита ping будет запущена на устройстве CPE, и отчет с результатами работы утилиты ping отобразится в нижней части области настройки.

Запуск утилиты traceroute

Чтобы запустить утилиту traceroute:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту traceroute.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Traceroute**.

   Отобразятся параметры утилиты traceroute.

4. В поле **IP-адрес назначения** введите IPv4-адрес, на который устройство CPE отправляет серию ICMP-запросов.

5. Если вы хотите, чтобы устройство CPE отправило серию ICMP-запросов с созданного сетевого интерфейса, в раскрывающемся списке **Интерфейс источника** выберите сетевой интерфейс.

6. Если вы хотите, чтобы при создании отчета с результатами работы утилиты traceroute устройство CPE преобразовывало IP-адреса в доменные имена с помощью DNS-сервера, установите флажок **Разрешать DNS-имена**. Вы можете указать DNS-сервер при создании или изменении сетевого интерфейса. IP-адреса, которые невозможно преобразовать в доменные имена, также отображаются в отчете. Этот флажок снят по умолчанию.

7. В поле **Таймаут проб (сек.)** введите время в секундах, по прошествии которого устройство CPE должно получить серию ICMP-ответов, чтобы считать серию ICMP-запросов успешной. Диапазон значений: от 1 до 30. Значение по умолчанию: `3`.

8. В поле **Максимум хопов** введите максимальное количество хопов для серии ICMP-запросов. Диапазон значений: от 1 до 60. Значение по умолчанию: `10`.

9. Нажмите на кнопку **Запустить**.

Утилита traceroute будет запущена на устройстве CPE, и отчет с результатами работы утилиты traceroute отобразится в нижней части области настройки.

Запуск утилиты tcpdump

В результате работы утилиты tcpdump генерируется отчет с захваченным трафиком. При повторном запуске утилиты tcpdump отчет перезаписывается. Вы можете скачать отчет, чтобы не потерять его.

Использование утилиты tcpdump создает дополнительную нагрузку на центральный процессор устройства CPE.

Чтобы запустить утилиту tcpdump:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту tcpdump.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Tcpdump**.

   Отобразятся параметры утилиты tcpdump.

4. В раскрывающемся списке **Сетевой интерфейс для захвата** выберите созданный сетевой интерфейс, на котором вы хотите захватывать трафик.

5. В раскрывающемся списке **Направление** выберите направление трафика, который вы хотите захватывать:

   - **Входящее** – захватывать входящий трафик.
   - **Исходящее** – захватывать исходящий трафик.
   - **Входящее/исходящее** – захватывать входящий и исходящий трафик. Это значение выбрано по умолчанию.

6. Если вы хотите, чтобы при создании отчета с захваченным трафиком устройство CPE преобразовывало IP-адреса в доменные имена с помощью DNS-сервера, установите флажок **Разрешать DNS-имена**. Вы можете указать DNS-сервер при создании или изменении сетевого интерфейса. IP-адреса, которые невозможно преобразовать в доменные имена, также помещаются в отчет. Этот флажок снят по умолчанию.

7. Если вы хотите использовать фильтр для захвата трафика, в поле **Фильтр tcpdump** введите синтаксис фильтра. Максимальная длина фильтра: 1024 символа. Например, вы можете использовать следующие фильтры:

   - `icmp` – захватывать только пакеты трафика протокола ICMP.
   - `host 1.2.3.4 and (port 80 or 443)` – захватывать только пакеты трафика с IPv4-адресом 1.2.3.4 и TCP-портом 80 или 443 источника или назначения.
   - `tcp[13] & 2 != 0` – захватывать только пакеты трафика TCP SYN.

   Более подробную информацию о фильтрах трафика можно получить из официальной документации tcpdump.

8. В поле **Максимальное время захвата (сек.)** введите время в секундах, по прошествии которого прекращается захват трафика. Диапазон значений: от 10 до 600. Значение по умолчанию: `30`.

9. В поле **Максимум захваченных пакетов** введите количество пакетов трафика, при котором прекращается захват трафика. Диапазон значений: от 1 до 10 000. Значение по умолчанию: `1000`.

   Захват трафика прекращается по прошествии времени, указанного в поле **Максимальное время захвата (сек.)**, или при захвате количества пакетов трафика, указанного в поле **Максимум захваченных пакетов**.

10. Нажмите на кнопку **Запустить**.

    Утилита tcpdump будет запущена на устройстве CPE, и будет сгенерирован отчет с захваченным трафиком.

Запуск утилиты iperf

В результате работы утилиты iperf генерируется отчет с результатами диагностики производительности сети. При повторном запуске утилиты iperf отчет перезаписывается. Вы можете скачать отчет, чтобы не потерять его.

Чтобы запустить утилиту iperf:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту iperf.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Iperf**.

   Отобразятся параметры утилиты iperf.

4. Укажите, в каком режиме вы хотите использовать утилиту iperf на устройстве CPE, выбрав один из следующих вариантов:

   - **Сервер** – использовать устройство CPE как iperf-сервер.
   - **Клиент** – использовать устройство CPE как iperf-клиент.

5. Если вы выбрали вариант **Сервер**, настройте iperf-сервер:

   a. В поле **Порт** введите номер порта TCP или UDP iperf-сервера. Диапазон значений: от 1001 до 65 535. Значение по умолчанию: `7777`.

   b. В поле **Интервал отчетов (сек.)** введите интервал времени в секундах для записи строчек в отчет. Диапазон значений: от 0 до 60. Значение по умолчанию: `3`.

   c. Если вы не хотите создавать отчет с результатами диагностики производительности сети, установите флажок **Без отчета**. Этот флажок снят по умолчанию.

   d. В блоке **Формат отчетов** выберите формат результатов диагностики производительности сети в отчете:

      - **Кбит/сек**. Это значение выбрано по умолчанию.
      - **Мбит/сек**.
      - **Кбайт/сек**.
      - **Мбайт/сек**.

   e. В поле **Запустить сервер на (сек.)** введите время работы iperf-сервера в секундах. Диапазон значений: от 60 до 3600. Значение по умолчанию: `300`.

6. Если вы выбрали вариант **Клиент**, настройте iperf-клиент:

   a. В поле **IP сервера** введите IPv4-адрес iperf-сервера, к которому подключается iperf-клиент.

   b. В поле **Порт** введите номер порта TCP или UDP iperf-сервера, к которому подключается iperf-клиент. Диапазон значений: от 1001 до 65 535. Значение по умолчанию: `7777`.

   c. В поле **Интервал отчетов (сек.)** введите интервал времени в секундах для записи строчек в отчет с результатами диагностики производительности сети. Диапазон значений: от 0 до 60. Значение по умолчанию: `3`.

   d. Если вы хотите не создавать отчет с результатами диагностики производительности сети, установите флажок **Без отчета**. Этот флажок снят по умолчанию.

   e. В блоке **Формат отчетов** выберите формат результатов диагностики производительности сети в отчете:

      - **Кбит/сек**. Это значение выбрано по умолчанию.
      - **Мбит/сек**.
      - **Кбайт/сек**.
      - **Мбайт/сек**.

   f. В поле **Запустить клиент на (сек.)** введите время работы iperf-клиента в секундах. Диапазон значений: от 60 до 3600. Значение по умолчанию: `60`.

   g. Укажите тип порта iperf-сервера, выбрав один из следующих вариантов:

      - **TCP**. Это значение выбрано по умолчанию.
      - **UDP**.

   h. В поле **Битрейт клиента** введите скорость передачи данных iperf-клиентом в одном из следующих форматов:

      - `<скорость в килобитах в секунду>k` или `<скорость в килобитах в секунду>K`

        Например, если вы вводите `10000K`, скорость передачи данных составляет 10 000 килобит в секунду.

      - `<скорость в мегабитах в секунду>m` или `<скорость в мегабитах в секунду>M`

        Например, если вы вводите `10M`, скорость передачи данных составляет 10 мегабит в секунду.

   i. В раскрывающемся списке **Направление теста** выберите направление трафика, который вы хотите использовать для измерения производительности сети:

      - **Клиент-сервер** – использовать трафик, который iperf-клиент передает iperf-серверу. Это значение выбрано по умолчанию.
      - **Сервер-клиент** – использовать трафик, который iperf-сервер передает iperf-клиенту.
      - **Двунаправленный** – использовать трафик, который iperf-клиент передает iperf-серверу и iperf-сервер передает iperf-клиенту.

j. При необходимости в поле **Размер окна TCP (байт)** введите размер TCP-окна в байтах. Если вы оставляете это поле пустым, размер TCP-окна определяется автоматически.

k. При необходимости в поле **TCP MSS (байт)** введите максимальный размер сегмента TCP в байтах.

7. Нажмите на кнопку **Запустить**.

Утилита iperf будет запущена на устройстве CPE, и будет сгенерирован отчет с результатами диагностики производительности сети.

Вы можете перейти к работе с отчетами, нажав на кнопку **Перейти к файлам**.

Запуск утилиты sweep

Вы можете использовать утилиту sweep, чтобы очистить ARP-кеш, перезапустить процесс FRR (Free Range Routing), очистить таблицу NAT-сессий или перезапустить модем на устройстве CPE.

Перезапуск процесса FRR и очистка таблицы NAT-сессий могут привести к прекращению передачи трафика в течение нескольких секунд.

Чтобы запустить утилиту sweep:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, котором вы хотите запустить утилиту sweep.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Sweep**.

   Отобразятся параметры утилиты sweep.

4. Если вы хотите очистить ARP-кеш, выполните следующие действия:

   a. В блоке **ARP-кеш** выберите созданный сетевой интерфейс, на котором вы хотите очистить ARP-кеш. При необходимости очистить ARP-кеш на всех сетевых интерфейсах выберите **Все**.

   b. Нажмите на кнопку **Запустить**.

   ARP-кеш будет очищен на устройстве CPE.

5. Если вы хотите перезапустить процесс FRR, в блоке **Процесс FRR** нажмите на кнопку **Запустить**.

   Процесс FRR будет перезапущен на устройстве CPE.

6. Если вы хотите очистить таблицу NAT-сессий, в блоке **Таблица NAT-сессий** нажмите на кнопку **Запустить**. Вы можете настроить NAT на устройстве CPE с помощью межсетевого экрана.

   Таблица NAT-сессий будет очищена на устройстве CPE.

7. Если вы хотите перезапустить модем, в блоке **Модем** выберите модем в списке **Перезапустить модем** и нажмите на кнопку **Запустить**.

   Модем будет перезапущен на устройстве CPE.

Запуск утилиты OpenFlow dump

В результате работы утилиты OpenFlow dump генерируется отчет с запрошенными dump-flows и dump-groups. При повторном запуске утилиты OpenFlow dump отчет перезаписывается. Вы можете скачать отчет, чтобы не потерять его.

Чтобы запустить утилиту OpenFlow dump:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту OpenFlow dump.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → OpenFlow dump**.

   Отобразятся параметры утилиты OpenFlow dump.

4. Нажмите на кнопку **Запустить**.

Утилита OpenFlow dump будет запущена на устройстве CPE, и будет сгенерирован отчет с запрошенными dump-flows и dump-groups.

Вы можете перейти к работе с отчетами, нажав на кнопку **Перейти к файлам**.

Сброс сессий BGP/OSPF

Вы можете выполнять команды сброса/очистки сессий BGP и OSPF на устройстве CPE. Для запуска команд необходимо создать запрос на очистку, который состоит из одной или нескольких команд очистки (`clear`-команд).

Чтобы создать и запустить запрос на очистку:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите выполнить команды очистки.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Сброс BGP/OSPF**.

   Отобразятся параметры создания команд очистки.

4. Нажмите на кнопку **Создать**.

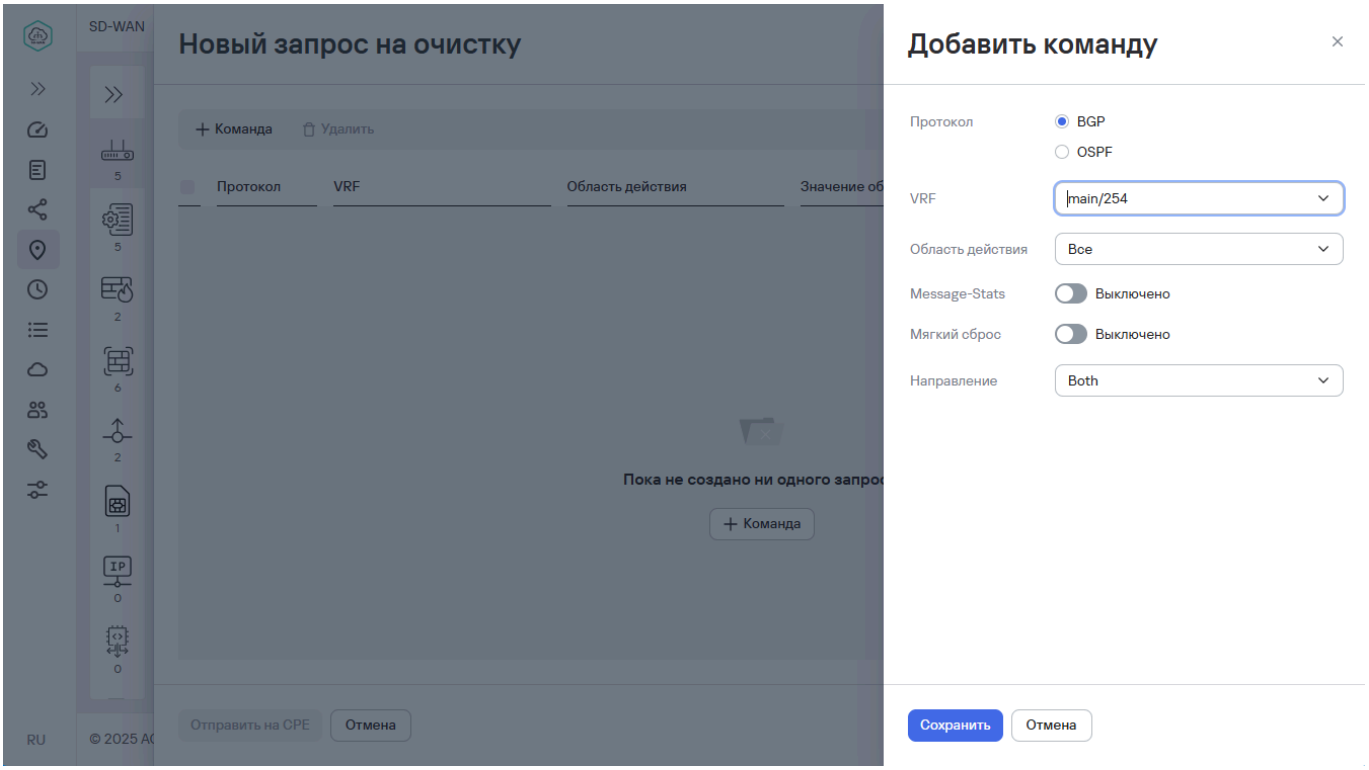
   Откроется область создания запроса на очистку с таблицей, где отображаются создаваемые команды очистки.

5. С помощью кнопки **Создать** добавьте одну или несколько команд:

   a. В области создания команды в поле **Протокол** выберите нужный протокол (**BGP** или **OSPF**).

   b. Укажите необходимые параметры команды очистки для выбранного протокола.

   c. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры команды.

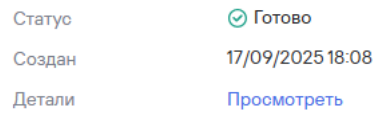


Добавление команды clear

Команда будет добавлена в таблицу. При необходимости вы можете выбрать команду в таблице и удалить ее с помощью кнопки **Удалить**.

6. Нажмите на кнопку **Отправить на CPE**.

Созданный запрос на очистку с набором команд будет отправлен на устройство CPE, и команды будут выполнены поочередно. Вы можете просмотреть статус выполнения последнего запроса и его подробности в блоке **Статус последнего запроса на очистку**.



Статус последнего запроса на очистку

Работа с отчетами

Отчеты генерируются в результате работы утилит tcpdump, iperf и OpenFlow dump. Для просмотра таблицы отчетов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Утилиты → Файлы**. Информация об отчетах отображается в следующих столбцах таблицы:

- **Тип** – формат отчета.
- **Создан** – дата и время создания отчета.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Скачивание отчета

Чтобы скачать отчет:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, с которого вы хотите скачать отчет.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Файлы**.

   Отобразится таблица отчетов.

4. Нажмите на кнопку **Загрузить** рядом с отчетом, который вы хотите скачать.

На ваше локальное устройство сохранится файл отчета.

Удаление отчета

Удаленные отчеты невозможно восстановить.

Чтобы удалить отчет:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите удалить отчет.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Файлы**.

   Отобразится таблица отчетов.

4. Нажмите на кнопку **Удалить** рядом с отчетом, который вы хотите удалить.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Отчет будет удален и перестанет отображаться в таблице.

Выполнение задач на устройствах CPE

Kaspersky SD-WAN поддерживает выполнение задач на устройствах CPE в указанное вами время. Вы можете использовать теги, чтобы сгруппировать устройства CPE, на которых вы хотите выполнить задачу.

Существуют следующие типы задач:

- Запланированный запуск скриптов на устройствах CPE.
- Запланированное обновление прошивки на выбранных вручную устройствах CPE и на устройствах CPE с указанными тегами.
- Запланированное обновление параметров CPE.

Когда вы создаете задачу, для ее выполнения используется часовой пояс виртуальной машины, на которой развернут оркестратор. Например, если вы запланировали запуск скрипта на устройстве CPE на 14:00, скрипт будет запущен в 14:00 по часовому поясу оркестратора, даже если время по часовому поясу устройства CPE – 18:00.

Мы рекомендуем учитывать следующие особенности при работе с задачами:

- Допускается 10-секундная погрешность во времени при выполнении задачи.
- При наличии нескольких задач они выполняются одновременно. Если оркестратор не может выполнить все задачи одновременно, они выполняются в порядке создания.
- При удалении шаблона CPE автоматически удаляются все связанные с ним задачи.
- При удалении устройства CPE автоматически удаляются все связанные с ним задачи.
- При удалении скрипта, связанного с задачами, вам нужно дополнительно подтвердить это действие. Если вы подтверждаете действие, скрипт удаляется и не может быть запущен в рамках созданных задач.
- Создание задач запланированного обновления параметров CPE недоступно из раздела меню **Планировщик**. Вы можете запланировать обновление только из области настройки конкретного устройства CPE.
- При наличии запланированной задачи изменения параметров устройства CPE редактирование связанного с этим устройством шаблона CPE блокируется до завершения обработки или отмены соответствующей задачи.

Задачи, которые еще не были выполнены, можно выполнить вручную.

Вы можете посмотреть таблицу задач в разделе **Планировщик**. Информация о задачах отображается в следующих столбцах таблицы:

- **ID** – идентификатор задачи.
- **Имя** – имя задачи.
- **Пользователь** – имя пользователя, который создал задачу.
- **Создан** – дата и время создания задачи.
- **Статус** – статус задачи:
  - **Выполнено** – задача успешно выполнена.
  - **Ошибка** – при выполнении задачи возникла ошибка.
  - **В ожидании** – задача помещена в базу данных оркестратора и ожидает выполнения.
  - **В очереди** – задача находится в очереди на выполнение.
  - **Выполняется** – задача выполняется.
- **Запланировано** – дата и время выполнения задачи.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание задачи

Чтобы создать задачу:

1. В меню перейдите в раздел **Планировщик**.

   Отобразится таблица запланированных задач.

2. В верхней части страницы нажмите на кнопку **+ Задача**.

3. В верхней части открывшейся боковой панели в списке **Тип** выберите тип задачи.

   Для создания задач из меню **Планировщик** доступны следующие типы задач:

   - Запуск скрипта;
   - Обновление прошивки.

   Задача с типом **Обновление параметров** создается, когда вы выполняете отложенное сохранение параметров в области настройки CPE с помощью кнопки **Запланированное сохранение**.

4. Укажите параметры задачи. Описание параметров задач см. в следующих инструкциях:

   - Запланированный запуск скриптов на устройствах CPE.
   - Запланированное обновление прошивки на устройствах CPE с указанными тегами.

5. Нажмите на кнопку **Создать**.

Задача будет создана и отобразится в таблице.

Выполнение задачи вручную

Чтобы вручную выполнить задачу:

1. В меню перейдите в раздел **Планировщик**.

   Отобразится таблица запланированных задач.

2. Если вы хотите вручную выполнить отдельную задачу, выполните следующие действия:

   a. Нажмите на задачу, которую вы хотите выполнить вручную.

      Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

   b. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Выполнить сейчас**.

3. Если вы хотите вручную выполнить несколько задач, выполните следующие действия:

   a. Установите флажки рядом с задачами, которые вы хотите выполнить вручную.

   b. В верхней части таблицы нажмите на кнопку **Действия** → **Выполнить сейчас**.

4. В открывшемся окне подтверждения нажмите на кнопку **Выполнить сейчас**.

Задачи будут выполнены, и их статус в столбце **Статус** изменится на **Выполнено**.

Удаление задачи

Удаленные задачи невозможно восстановить.

Чтобы удалить задачу:

1. В меню перейдите в раздел **Планировщик**.

   Отобразится таблица запланированных задач.

2. Если вы хотите удалить отдельную задачу, выполните следующие действия:

   a. Нажмите на задачу, которую вы хотите удалить.

      Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

   b. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

3. Если вы хотите удалить несколько задач, выполните следующие действия:

   a. Установите флажки рядом с задачами, которые вы хотите удалить.

   b. В верхней части таблицы нажмите на кнопку **Действия** → **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Задачи будут удалены и перестанут отображаться в таблице.

Проверки CPE

Проверка целостности

Эта функция позволяет автоматически или вручную проверять целостность критически важных файлов, отвечающих за работу системы и межсетевого экрана в частности, сравнивая их с эталонными контрольными суммами. Она может обнаруживать несанкционированные изменения и гарантирует, что системные сценарии и исполняемые файлы соответствуют выпущенной прошивке.

Вы можете запускать проверку по требованию или настроить проверку по расписанию.

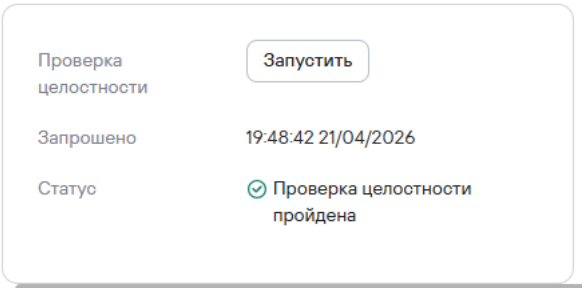
Запуск проверки целостности по требованию

Проверку целостности по требованию можно запускать только на устройстве CPE.

Чтобы запустить проверку целостности по требованию:

1. Перейдите в меню оркестратора **Шаблоны CPE** и выберите шаблон
2. Откройте раздел **SD-WAN** и перейдите на вкладку **Проверки CPE**.
3. В блоке **Ручная проверка** нажмите кнопку **Запустить** для секции **Проверка целостности**.

На устройстве CPE запустится утилита, которая выполнит проверку и выведет информацию в системный журнал устройства CPE. При этом в блоке **Ручная проверка** в секции **Проверка целостности** будет показана дата и время запуска проверки. После того, как проверка завершится, в поле **Статус** будет показан результат выполнения проверки.



Результат проверки целостности на устройстве CPE

Также статус и результат проверки отображается в области настройки параметров устройства CPE в разделе **Главное** в блоке **Внеполосное управление**. После запуска задача **Проверка целостности** имеет статус **Выполнение**. Далее, в зависимости от результатов работы утилиты, CPE передает оркестратору статус Успешно или Ошибка.

Запуск проверки целостности по расписанию

Вы можете настроить запуск проверки целостности по расписанию как в шаблоне CPE, так и на устройстве CPE.

Чтобы настроить запуск проверки целостности по расписанию:

1. Перейдите в меню оркестратора Шаблоны CPE, выберите шаблон, далее перейдите в пункт меню SD-WAN → вкладка «Проверки CPE» и нажмите на переключатель «Проверка целостности» в секции «Расписание проверок».
2. На CPE нужно будет предварительно нажать на переключатель «Переопределить» .
3. Установите интервал между проверками. В выпадающем списке доступны значения: 1, 2, 3 ,4 , 6, 8 и 12 часов. Значение интервала по умолчанию - 8
4. При необходимости включите блокировку транзитного трафика на устройстве CPE при неудачных проверках с помощью переключателя **Блокировать передачу трафика при неудачных проверках**.

На устройстве CPE с указанной периодичностью будет запускаться утилита, которая выполняет проверку и выводит информацию в системный журнал устройства CPE.

Также статус и результат проверки отображается в области настройки параметров устройства CPE в разделе **Главное** в блоке **Внеполосное управление**. После запуска задача **Проверка целостности** имеет статус **Выполнение**. Далее, в зависимости от результатов работы утилиты, CPE передает оркестратору статус Успешно или Ошибка.

Дополнительно можно заблокировать передачу трафика при неудачных проверках.

Самотестирование межсетевого экрана

Эта функция позволяет автоматически или вручную проверять работоспособность межсетевого экрана на CPE (осуществлять самотестирование).

Вы можете запускать проверку по требованию или настроить проверку по расписанию.

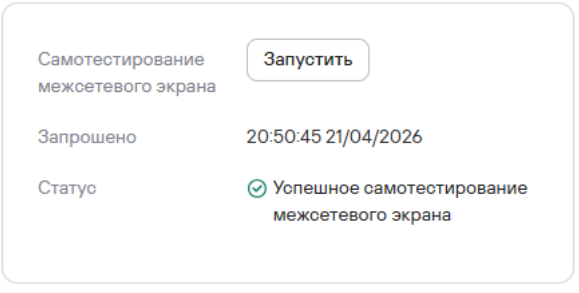
Запуск самотестирования межсетевого экрана по требованию

Вы можете запускать самотестирование межсетевого экрана по требованию только на устройстве CPE.

Чтобы запустить проверку целостности по требованию:

1. Перейдите в меню оркестратора **CPE** и выберите устройство.
2. Откройте раздел **SD-WAN** и перейдите на вкладку **Проверки CPE**.
3. В блоке **Ручная проверка** нажмите кнопку **Запустить** для секции **Самотестирование межсетевого экрана**.

На устройстве CPE запустится скрипт, который выполняет проверку и выводит информацию в системный журнал устройства CPE. При этом в блоке **Ручная проверка** в секции **Самотестирование межсетевого экрана** будет показана дата и время запуска проверки. После того, как проверка завершится, в поле **Статус** будет показан результат выполнения проверки.



Результат самотестирования межсетевого экрана на устройстве CPE

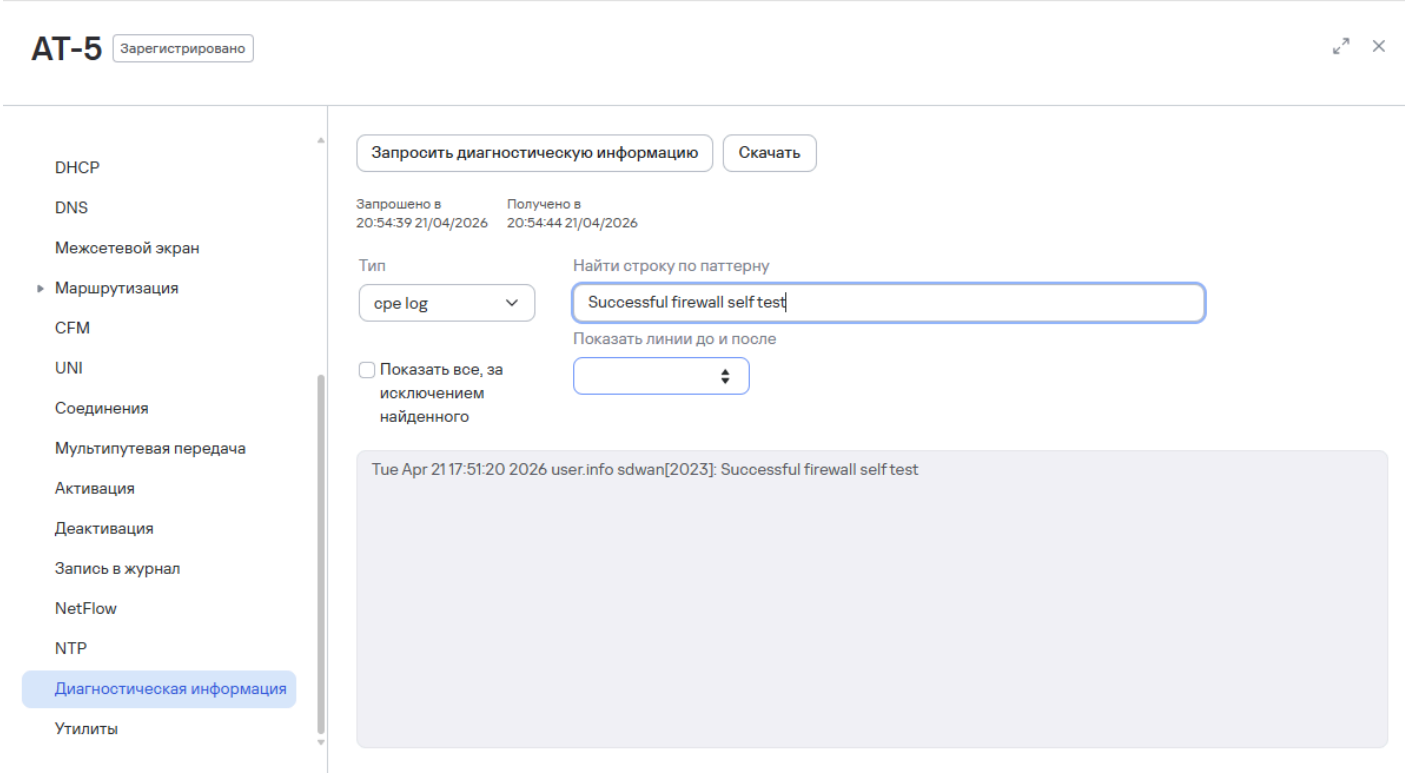
Также статус и результат проверки отображается в области настройки параметров устройства CPE в разделе **Главное** в блоке **Внеполосное управление**. После запуска задача **Самотестирование межсетевого экрана** имеет статус **Выполнение**. Далее, в зависимости от результатов работы утилиты, CPE передает оркестратору статус Успешно или Ошибка.

Скрипт проверяет, запущен ли сервис межсетевого экрана.

Вы можете проверить статус выполнения задачи в системном журнале CPE. Для этого:

1. Перейдите в раздел меню **Диагностическая информация**
2. Нажмите кнопку **Запросить диагностическую информацию** и дождитесь выполнения запроса.
3. Выберите в выпадающем списке **Тип** значение `cpe log`.

Если самотестирование межсетевого экрана было выполнено успешно, в системном журнале CPE будет присутствовать запись типа `user.info sdwan` с сообщением `Successful firewall self test`.



Запись в журнале устройства CPE об успешном завершении самотестирования межсетевого экрана

Запуск самотестирования межсетевого экрана по расписанию

Вы можете настроить запуск самотестирования межсетевого экрана по расписанию как в шаблоне CPE, так и на устройстве CPE.

Чтобы настроить запуск самотестирования межсетевого экрана по расписанию:

1. Перейдите в меню оркестратора Шаблоны CPE, выберите шаблон, далее перейдите в пункт меню SD-WAN → вкладка **Проверки CPE** и включите переключатель **Самотестирование межсетевого экрана** в блоке **Расписание проверок**.
2. На CPE нужно будет предварительно нажать на переключатель **Переопределить**.
3. Установите интервал между проверками. В выпадающем списке доступны значения: 1, 2, 3 ,4 , 6, 8 и 12 часов. Значение интервала по умолчанию - 8.
4. При необходимости включите блокировку транзитного трафика на устройстве CPE при неудачных проверках с помощью переключателя **Блокировать передачу трафика при неудачных проверках**.

На устройстве CPE с указанной периодичностью будет запускаться скрипт, который проводит проверку и выводит информацию в системный журнал CPE.

Статус и результат проверки отображается в области настройки параметров устройства CPE в разделе **Главное** в блоке **Внеполосное управление**. После запуска задача **Проверка целостности** имеет статус **Выполнение**. Далее, в зависимости от результатов работы утилиты, CPE передает оркестратору статус Успешно или Ошибка.

Неуспешные проверки также отображаются во вкладке **Проблемы** меню CPE.

Блокировка трафика при ошибках самотестирования и проверки целостности

Эта функция предназначена для блокирования проходящего трафика в случае, если не пройдены проверки самотестирования и целостности критически важных системных файлов и скриптов на устройстве CPE. Она дополняет функции самотестирования и проверки целостности firewall и настраивается совместно с ними.

Вы можете включить блокировку проходящего трафика совместно с проверками по расписанию.

Для настройки блокировки трафика на устройстве CPE перейдите в меню оркестратора CPE, выберите устройство, перейдите в пункт меню **SD-WAN** → вкладка **Проверки CPE**. Убедитесь, что в секции Расписание проверок включены обе функции Проверка целостности и Самотестирование межсетевого экрана.

Если необходимо, включите переключатель Переопределить для модификации функций проверок.

Теперь вы можете включить блокировку трафика (Блокировать передачу трафика при неудачных проверках).

Не забудьте скорректировать временной интервал между проверками.

Для настройки блокировки трафика в шаблоне CPE перейдите в меню оркестратора Шаблоны CPE, выберите шаблон, далее перейдите в пункт меню SD-WAN → вкладка Проверки CPE. В секции Расписание проверок включите функции Проверка целостности и Самотестирование межсетевого экрана.

Теперь вы можете включить блокировку трафика (Блокировать передачу трафика при неудачных проверках).

Оркестратор покажет всплывающее окно: Если любая из проверок закончится неудачей, прохождение транзитного трафика будет заблокировано на всех устройствах CPE, использующих этот шаблон. Вы уверены. что хотите продолжить?

Выберите Да, продолжить, если согласны.

Также Вы можете сформировать индивидуальные шаблоны для отдельных устройств CPE с включенной функцией блокировки.

Не забудьте скорректировать временной интервал между проверками.

Если какая-либо из проверок пройдет неуспешно, CPE заблокирует прохождение транзитного трафика (трафик между интерфейсами). При этом связь между CPE и оркестратором не нарушается, что позволяет вносить изменения в конфигурацию и управлять устройством.

CPE сообщит оркестратору о блокировке трафика, оркестратор покажет соответствующее всплывающее окно для этого CPE:

"Прохождение транзитного трафика на CPE заблокировано. Чтобы определить причину воспользуйтесь разовыми проверками. Если проблема в самотестировании firewall, то перезагрузите CPE. Если проблема в проверке целостности, то восстановите прошивку CPE с помощью обновления."

Когда прохождение транзитного трафика на CPE будет вновь разрешено, оркестратор уберет всплывающее окно.

Вы можете проверить статус выполнения проверок и блокировки трафика в системном журнале CPE следующим образом. Перейдите в раздел меню Диагностическая информация, нажмите кнопку Запросить диагностическую информацию, дождитесь выполнения запроса и выберите cpe log в выпадающем списке Тип. В системном журнале CPE вы увидите такие записи:

- тип `user.crit.fwblock`, сообщение `Firewall self test failed. Traffic forwarding blocked`.

  Самотестирование межсетевого экрана выполнено неудачно. Переадресация трафика заблокирована.

- тип `user.crit.integrityblock`, сообщение `Firewall integrity check failed. Traffic forwarding blocked`.

  Проверка целостности не пройдена. Переадресация трафика заблокирована.

- тип `user.info.checksuccess`, сообщение `Verification was successful`.

  Проверки прошли успешно. Прохождение транзитного трафика разрешено.

Аудит событий безопасности

На оркестраторе Kaspersky SD-WAN и устройствах CPE могут происходить события, имеющие важность с точки зрения информационной безопасности: авторизация пользователей, изменение конфигурации шаблонов или устройств, взаимодействие с внешними системами и т.п. Такие события называются *событиями безопасности* и требуют повышенного внимания со стороны администраторов сети. Для централизованной фиксации событий безопасности в Kaspersky SD-WAN предусмотрен аудит событий безопасности. События безопасности, возникающие на оркестраторе, регистрируются в журналах Docker контейнера, в котором запущен оркестратор. События безопасности, возникающие на устройствах CPE, регистрируются в системных журналах устройств. После регистрации события безопасности отправляются на сервер syslog, указанный в файле конфигурации при развертывании решения. Для более удобной обработки событий вы можете настроить в качестве syslog-сервера внешний коллектор SIEM (например, Kaspersky Unified Monitoring and Analysis Platform, далее также KUMA). Для некоторых событий безопасности вы также можете настроить, какие именно из них записывать в журнал аудита, а также степень подробности записи (регистрировать ли только сам факт события или также его детали).

Этот раздел содержит инструкции по настройке аудита событий безопасности оркестратора и устройств CPE и настройке внешнего коллектора KUMA.

Настройка регистрации событий безопасности для аудита

События безопасности регистрируются и хранятся в журналах на оркестраторе и на устройствах CPE. Для полноценной работы с журналами аудита вам необходимо настроить отправку событий на внешний syslog-сервер. Мы рекомендуем использовать в качестве syslog-сервера решение Kaspersky Unified Monitoring and Analysis Platform (далее KUMA).

Параметры syslog для отправки записей журналов оркестратора необходимо указать в конфигурационном файле перед развертыванием решения. Если вы захотите изменить параметры, например, указать другой адрес syslog-сервера или CA-сертификат, вам потребуется изменить конфигурационный файл и переустановить решение. Если вы хотите использовать защищенное соединение для syslog-сервера, вам необходимо заранее получить CA-сертификат

Чтобы настроить регистрацию событий безопасности для аудита:

1. Если вы хотите использовать в качестве syslog-сервера коллектор KUMA:

   a. Разверните и настройте коллектор KUMA, как описано в инструкции Настройка коллектора KUMA для обработки событий безопасности.

   b. Сохраните CA-сертификат сервера KUMA, чтобы использовать его для шифрования syslog-сообщений с помощью TLS:

      1. Откройте веб-интерфейс KUMA.

      2. В левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **CA-сертификат Microservice**.

2. Настройте отправку записей журналов оркестратора на syslog-сервер в конфигурационном файле для развертывания решения:

   a. Подготовьте конфиграционный файл и заполните в нем основные параметры для развертывания решения.

   b. В блоке `external.orc` заполните следующие параметры syslog-сервера:

- `syslog_server_address`

  Укажите веб-адрес syslog-сервера, на который Docker-контейнеры оркестратора будут отправлять записи журналов. Значение указывается в формате `<протокол>://<адрес хоста>:<номер порта>`. В качестве адреса хоста можно указать IP-адрес или FQDN хоста.

  Если вы хотите, чтобы передача syslog-сообщений шифровалась с помощью TLS, в качестве протокола укажите `tcp+tls`.

  Пример:

  `tcp+tls://my-syslog-server:1514`

  > Если вы указываете внешний syslog-сервер, например, коллектор KUMA, отключите опцию развертывания отдельного контейнера для встроенного syslog-сервера. Для этого укажите в параметре `external.syslog.state` значение `disabled`.

- `secure_syslog`

  Укажите `true`, если необходимо шифровать передачу записей журналов на сервер, или `false`, если шифрование не требуется.

  Если вы указали `true`, сообщения syslog будут оправляться по TCP и шифроваться с помощью TLS. Для работы TLS необходимо дополнительно указать путь к CA-сертификату, которым подписан сертификат syslog-сервера, в переменной `syslog_server_ca_cert_file_path`.

- `syslog_server_ca_cert_file_path`

  Укажите абсолютный путь к файлу CA-сертификата, которым подписан сертификат syslog-сервера. Параметр обязателен, если для переменной `secure_syslog` вы указали `true`.

  Если CA-сертификат syslog-сервера был выписан на доменное имя, то для использования TLS-шифрования необходимо указать адрес сервера в параметре `syslog_server_address` в формате FQDN. Это доменное имя должно разрешаться через DNS-сервер, указанный при настройке DNS на устройстве CPE.

- `syslog_format`

Укажите формат журналов, который необходимо использовать для отправки syslog-сообщений. Возможные значения:

- `rfc3164` – формат, совместимый с RFC 3164.
- `rfc5424` – формат, совместимый с RFC 5424.
- `rfc5424micro` – формат, совместимый с RFC 5424 с увеличенной точностью меток времени до микросекунд.

Если в качестве syslog-сервера вы хотите использовать коллектор KUMA, укажите значение `rfc3164`.

3. Выполните развертывание решения.

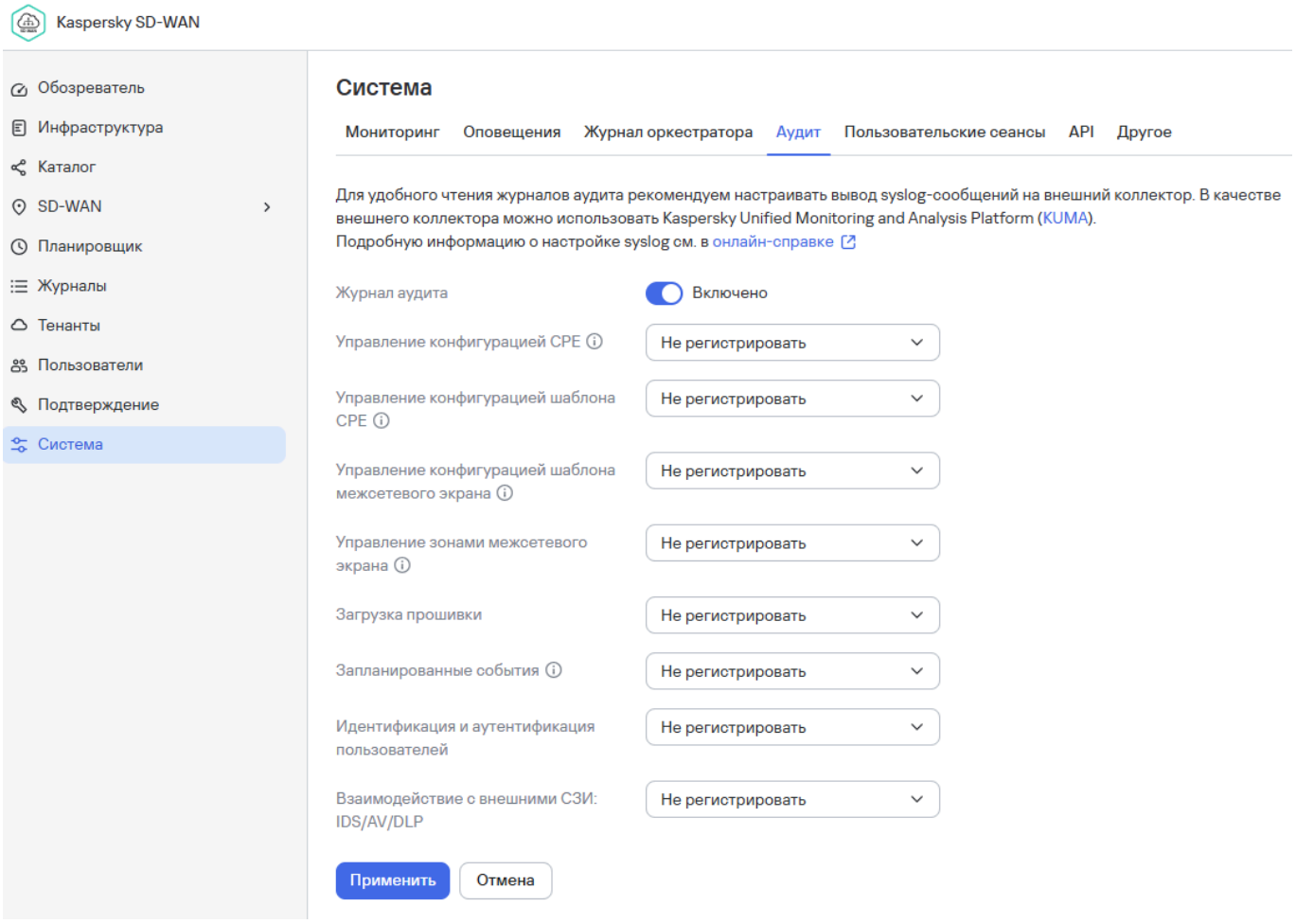
   Контейнеры оркестратора будут развернуты с параметрами syslog-сервера, указанными в конфигурационном файле.

4. Войдите в веб-интерфейсе оркестратора для дальнейшей настройки параметров аудита.

5. Выберите, какие события безопасности оркестратора должны регистрироваться в журнале аудита:

   a. Перейдите в раздел **Система** → **Аудит**.

      Откроется список областей аудита, для которых можно включить регистрацию событий безопасности на оркестраторе. Событие безопасности возникает, если изменяется состояние области аудита, например, изменяются параметры на устройстве или в шаблоне CPE или происходит вызов API внешней системой защиты информации.



Настройка журнала аудита для событий безопасности оркестратора

   a. Включите ведение журнала аудита с помощью переключателя **Журнал аудита**.

      При каждом включении или выключении этого параметра в журнале аудита регистрируется событие с кодом `SYS-AUD`.

   b. Для каждой категории событий безопасности, которое необходимо регистрировать, выберите в выпадающем списке режим регистрации:

      - **Стандартный** (регистрировать возникновение события в выбранной области аудита)
      - **Расширенный** (регистрировать подробную информацию о событии в выбранной области аудита, например, старое и новое значение при изменении параметра и т.п. Доступно не для всех областей аудита).

   c. Сохраните изменения с помощью кнопки **Применить**.

События безопасности, возникающие в выбранных областях аудита, будут регистрироваться в журнале аудита и передаваться на syslog-сервер, который вы указали в конфигурационном файле при развертывании решения.

Подробный событий безопасности, регистрируемых на оркестраторе, можно найти в статье Перечень событий безопасности, регистрируемых на оркестраторе и устройствах CPE.

6. Настройте syslog-сервер для журналов на устройствах CPE:

   a. В веб-интерфейсе оркестратора перейдите к устройствам или шаблонам CPE, на которых вы хотите настроить syslog-сервер для отправки записей журналов.

   b. С помощью инструкции Настройка журналов на устройствах CPE настройте параметры syslog-сервера. Если вы хотите использовать в качестве syslog-сервера коллектор KUMA, загрузите на устройства сохраненный ранее CA-сертификат сервера.

   События безопасности, возникающие на устройствах CPE, будут передаваться на указанный syslog-сервер.

   Подробный событий безопасности, регистрируемых на устройствах CPE, можно найти в статье Перечень событий безопасности, регистрируемых на оркестраторе и устройствах CPE.

Перечень событий безопасности, регистрируемых на оркестраторе и устройствах CPE

Ниже представлен список событий безопасности, которые регистрируются в журнале аудита оркестратора.

Перечень событий безопасности, подлежащих регистрации

Код / Code	Событие / Event	Действие	Уровень Severity в логе / Severity	Уровень Severity события KUMA	Момент активации	Пример отображаемого событ
Журнал аудита (Audit logging)						
SYS-AUD	Started	Включение подсистемы аудита	info	low	При нажатии: Save	Message: Code Event: Username:$username($t ...], Extended: [$code ...], OrcVersion:$orcversion SYS-AUD Started: Username:admin(tenant-1), U SDW-CPET, SDW-FWT, SDW-FWZ, SDW-FMW SYS-API], Extended: [], OrcVersion:3.0.0.release SYS-AUD Started: Username:admin(tenant-1), U [SDW-CPE, SDW-CPET, SDW-FWT, SDW-FWZ SYS-AUD Started: Username:admin(tenant-1), U SCH-FMWU, USR-USR, SYS-API], Extended: [SI FWZ], OrcVersion:3.0.0.release.1.cis.amd64
SYS-AUD	Stopped	Отключение подсистемы аудита	warn	medium	При нажатии: Save	Message: Code Event: Username:$username($t ...], Extended: [$code ...], OrcVersion:$orcversion SYS-AUD Stopped: Username:admin(tenant-1), U SDW-CPET, SDW-FWT, SDW-FWZ, SDW-FMW SYS-API], Extended: [], OrcVersion:3.0.0.release SYS-AUD Stopped: Username:admin(tenant-1), U [SDW-CPE, SDW-CPET, SDW-FWT, SDW-FWZ SYS-AUD Stopped: Username:admin(tenant-1), U SCH-FMWU, USR-USR, USR-PERM, SYS-API], E FWT, SDW-FWZ], OrcVersion:3.0.0.release.1.cis.a

SYS-AUD	Error	Невозможно запустить подсистему аудита	warn	medium	Сразу при возникновении	Message: Code Event: Standard: [$code ...], Ext OrcVersion:$orcversion, $ErrorMessage SYS-AUD Error: Standard: [SDW-CPE, SDW-CP SCH-FMWU, USR-USR, USR-PERM, SYS-API], E OrcVersion:3.0.0.release.1.cis.amd64, $ErrorMess SYS-AUD Error: Standard: [], Extended: [SDW-C OrcVersion:3.0.0.release.1.cis.amd64, $ErrorMess SYS-AUD Error: Standard: [SDW-FMW, SCH-FM Extended: [SDW-CPE, SDW-CPET, SDW-FWT, S OrcVersion:3.0.0.release.1.cis.amd64, $ErrorMess
Управление конфигурацией CPE (CPE configuration management)						
SDW-CPE	Any	Любое изменение в любых разделах CPE, которое не попадает под специализируемые разделы описанных ниже.	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name, C SDW-CPE Any: Username:admin(tenant-1), User CTenant:tenant-1, OrcVersion:3.0.0.release.1.cis.a
SDW-CPE	AnyError	Любое изменение в любых разделах CPE, которое не попадает под специализируемые разделы описанных ниже с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE AnyError: CPE:vCPE1, Template:vCPI
SDW-CPE	Create	Создание CPE	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name. SDW-CPE Create: Username:admin(tenant-1), U Template:vCPE1, CTenant:tenant-1.
SDW-CPE	CreateError	Создание CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE CreateError: CPE:vCPE1, Template:v
SDW-CPE	Registration	Регистрация CPE	info	low	Когда CPE перешла в статус: Activate	Standard/Extended: Code Event: CPE:$name, T SDW-CPE Registration: CPE:vCPE1, Template:v
SDW-CPE	RegistrationError	Регистрация CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE RegistrationError: CPE:vCPE1, Templ $ErrorMessage
SDW-CPE	Delete	Удаление CPE	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name SDW-CPE Delete: Username:admin(tenant-1), U Template:vCPE1, TTenant:tenant-1, CTenant:ten
SDW-CPE	DeleteError	Удаление CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE DeleteError: CPE:vCPE1, Template:v
SDW-CPE	Disable	Отключение CPE	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name SDW-CPE Disable: Username:admin(tenant-1), U Template:vCPE1, TTenant:tenant-1, CTenant:ten
SDW-CPE	DisableError	Отключение CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE DisableError: CPE:vCPE1, Template:v
SDW-CPE	Enable	Включение CPE	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name SDW-CPE Enable: Username:admin(tenant-1), U Template:vCPE1, CTenant:tenant-1

SDW-CPE	EnableError	Включение CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE EnableError: CPE:vCPE1, Template:v
SDW-CPE-GEN	FirewallTemplate	Изменение шаблонов экземпляра CPE	info	low	При нажатии: Save	Standard: Code Event: Username:$username($t Template:$name, CTenant:$name, OrcVersion:$ SDW-CPE-GEN FirewallTemplate: Username:adı Template:vCPE1, CTenant:tenant-1, OrcVersion: Extended: Code Event: Username:$username(te Template:$name, CTenant:$name, OrcVersion:$ SDW-CPE-GEN FirewallTemplate: Username:adı Template:vCPE1, CTenant:tenant-1, OrcVersion: [Changed:Default firewall template>Default firev
SDW-CPE-GEN	FirewallTemplateError	Изменение шаблонов экземпляра CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE-GEN FirewallTemplateError: CPE:vCI $ErrorMessage
SDW-CPE-ENC	Encryption	Изменение шифрования канала на экземпляре CPE	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name, C [Changed:$state], SDW-CPE-ENC Encryption: Username:admin(te Template:vCPE1, CTenant:tenant-1, OrcVersion: [Changed:enabled || disabled]
SDW-CPE-ENC	EncryptionError	Изменение шифрования канала на экземпляре CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE-ENC EncryptionError: CPE:vCPE1, Te $ErrorMessage
SDW-CPE-SCR	Scripts	Запуск скриптов на экземпляре CPE	info	low	При нажатии: Run	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name, C $SriptName] SDW-CPE-SCR Scripts: Username:admin(tenar Template:vCPE1, CTenant:tenant-1, OrcVersion: [Run:custom_config]
SDW-CPE-SCR	ScriptsError	Запуск скриптов на экземпляре CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE-SCR ScriptsError: CPE:vCPE1, Temp $ErrorMessage

SDW-CPE-NET	Interface	Добавление/ Удаление/ Изменение зоны/IP адреса/ MAC адреса/QoS интерфейса на экземпляре CPE	info	low	При нажатии: Save	Standard: Code Event: Username:$username($t Template:$name, CTenant:$name, OrcVersion:$ SDW-CPE-NET Interface: Username:admin(tena Template:vCPE1, CTenant:tenant-1, OrcVersion:3 [Changed] Extended: Code Event: Username:$username($ Template:$name, CTenant:$name, OrcVersion:$ Deleted || Changed: GEN || QOS: $Detailed_char SDW-CPE-NET Interface: Username:admin(tena Template:vCPE1, CTenant:tenant-1, OrcVersion:3 [Added: GEN: Zone:lan, Bridge:false, Enable autc IPv4 address:10.1.1.1, IPv4 netmask:255.0.0.0, IPv4 broadcast:10.1.1.255, Override MAC:01:01:01:01:01:(Enable QoS:false, MaxRate:1000, BE(MinR):10, BI SDW-CPE-NET Interface: Username:admin(tena Template:vCPE1, CTenant:tenant-1, OrcVersion:3 [Deleted: GEN: Zone:lan, Bridge:false, Enable aut IPv4 address:10.1.1.1, IPv4 netmask:255.0.0.0, IPv4 broadcast:10.1.1.255, Override MAC:01:01:01:01:01:(Enable QoS:false, MaxRate:1000, BE(MinR):10, BI SDW-CPE-NET Interface: Username:admin(tena Template:vCPE1, CTenant:tenant-1, OrcVersion:3 [Changed: GEN: Zone: lan>lan(tenant-1), Bridge:f automatically:true>false, IPv4 input type: Manua 10.1.1.1>10.2.2.2, IPv4 netmask: 255.0.0.0>255.255.0. broadcast: 10.1.1.255>10.2.2.255, Override MAC: 0 Generate MAC: true>false, Changed: QOS: Enab BE(MaxR):90] Показываем изменение с/на при Change в GE Не отображается изменение с/на при Change параметры.
SDW-CPE-NET	InterfaceError	Добавление/ Удаление/ Изменение зоны/QoS интерфейса на экземпляре CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $alias, [GEN || QoS], $ErrorMessage SDW-CPE-NET InterfaceError: CPE:vCPE1, Tem [GEN], $ErrorMessage SDW-CPE-NET InterfaceError: CPE:vCPE1, Tem [QoS], $ErrorMessage

SDW-CPE-FW	Firewall	Изменение настроек МЭ на экземпляре CPE	info	low	При нажатии: Save	Standard: Code Event: Username:$username($t Template:$name, CTenant:$name, OrcVersion:$ SDW-CPE-FW Firewall: Username:admin(tenant Template:vCPE1, CTenant:tenant-1, OrcVersion: Extended: Code Event: Username:$username($ Template:$name, CTenant:$name, OrcVersion:$ GEN || RUL || ADVR || NAT || ZF || IPSET || DPI || ZO SDW-CPE-FW Firewall: Username:admin(tenant CTenant:tenant-1, OrcVersion:3.0.0.release.1.cis.a protection:Disable, Default INPUT action:REJEC SDW-CPE-FW Firewall: Username:admin(tenant CTenant:tenant-1, OrcVersion:3.0.0.release.1.cis.a Action:ACCEPT, IPset:null, IPv:IPv4, SrcZ:wan, Ds DstIP:3.3.3.3:4.4.4.4, Proto:icmp, + new rule), Dele IPset:null, IPv:IPv4, SrcZ:wan, DstZ: lan, SrcIP:11.11.1 rule), Changed: RUL: (Name:Allow-Ping, Action:D DstZ:null, SrcIP:null, DstIP:null, Proto:icmp, + new SDW-CPE-FW Firewall: Username:admin(tenant CTenant:tenant-1, OrcVersion:3.0.0.release.1.cis.a Name:Test, Ptags:null, Table:FILTER, Chain:INPUT rules,Start of table, DstIP:1.1.1.1, MakeAnEx:false, S Frag:false, MarkVal:null, MarkMask:null, TosVal:nu StrAlg:BM, StrRange:1-65535, StrHEX:false, Strl RecentProto:SET, RecentSec:null, RecentHit:nul new rule), Deleted: ADVR: (Status:On, Name:Tes (Status:Off, Name:ICMP ..., + new rule)] SDW-CPE-FW Firewall: Username:admin(tenant CTenant:tenant-1, OrcVersion:3.0.0.release.1.cis.a Proto:IP, SP-DestIP:1.1.1.1, SP-SrcZone:lan(tenant- DestZone:wan(tenant-1), + new rule), Deleted: NA DestIP:1.1.1.1, SP-SrcZone:lan(tenant-1), SP-SrcIP: DestZone:wan(tenant-1), + new rule), Changed: N DestIP:1.1.1.1, SP-SrcZone:lan(tenant-1), SP-SrcIP: DestZone:wan(tenant-1), + new rule)] SDW-CPE-FW Firewall: Username:admin(tenant template, Owner: admin(tenant-1), OrcVersion:3 (From:Any zone, To:mgmt,+ new rule), Deleted: Z Changed: ZF: (From:wan, To:lan,+ new rule)] SDW-CPE-FW Firewall: Username:admin(tenant CTenant:tenant-1, OrcVersion:3.0.0.release.1.cis.a Direction:Match source, Type:Set of subnets, Er rule), Deleted: IPSET: (Name:test, Direction:Matc EntryList:10.1.1.[1-254]/24,20.2.2.[1-5], + new rule) Direction:Match source, Type:Set of subnets, Er rule)] SDW-CPE-FW Firewall: Username:admin(tenant CTenant:tenant-1, OrcVersion:3.0.0.release.1.cis.a SDW-CPE-FW Firewall: Username:admin(tenant CTenant:tenant-1, OrcVersion:3.0.0.release.1.cis.a Input:ACCEPT, Output:ACCEPT, Forwarding:AC to PMTU:false, Drop logging:false, Networks:11.1.1 ZONE: (Name:RULE2, Input:ACCEPT, Output:AC Masquerading:false, MSS clamp to PMTU:false, 22.2.2.2/32, + new rule), Changed: ZONE: (Name:F Forwarding:REJECT, Masquerading:true, MSS cl Networks:11.1.1.1/32, 33.3.3.3/32, + new rule)] PKTmark: отображаются только включенные, и Не отображается изменение с/на при Change параметры.
SDW-CPE-FW	FirewallError	Изменение настроек МЭ на экземпляре CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T RUL || ADVR || NAT, ZF || IPSET || DPI || ZONE], $Er SDW-CPE-FW FirewallError: CPE:vCPE1, Templa || ADVR || NAT, ZF || IPSET || DPI || ZONE], $ErrorM

SDW-CPE-STR	StaticRoute	Добавление/ Удаление/ Изменение настроек статических маршрутов	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name, C Deleted || Changed: VRF:$vrf, Destination:$dest Gateway:$gateway, Interface:$interface, Metric Type:$type] SDW-CPET-STR StaticRoute: Username:admin(Template:vCPE1, CTenant:tenant-1, OrcVersion: VRF:main/254, Destination:10.1.1.1/255.0.0.0, Gate MTU:1500, AD:20, Type:unicast] SDW-CPET-STR StaticRoute: Username:admin(Template:vCPE1, CTenant:tenant-1, OrcVersion: VRF:main/254, Destination:10.1.1.1/255.0.0.0, Gate MTU:1500, AD:20, Type:unicast] SDW-CPET-STR StaticRoute: Username:admin(Template:vCPE1, CTenant:tenant-1, OrcVersion: VRF:yellow/100, Destination:10.2.2.2/255.255.0.0 Metric:10, MTU:1300, AD:10, Type:blackhole] Не отображается изменение с/на при Change параметры.
SDW-CPE-STR	StaticRouteError	Добавление/ Удаление/ Изменение настроек статических маршрутов с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPE-STR StaticRoute: CPE:vCPE1, Templ $ErrorMessage
Управление конфигурацией шаблона (CPE template configuration management)						
SDW-CPET	Any	Любое изменение в любых разделах CPE Template, которое не попадает под специализируемые разделы описанные ниже.	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us Template:$name, Owner:$owner, OrcVersion:$o SDW-CPET Any: Username:admin(tenant-1), Use Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am
SDW-CPET	AnyError	Любое изменение в любых разделах CPE Template, которое не попадает под специализируемые разделы описанные ниже с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: Template:$na SDW-CPET AnyError: Template:vCPE1, Owner:t
SDW-CPET-ENC	Encryption	Изменение шифрования канала в шаблоне CPE	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us Template:$name, Owner:$owner, OrcVersion:$o SDW-CPET-ENC Encryption: Username:admin(t Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am
SDW-CPET-ENC	EncryptionError	Изменение шифрования канала в шаблоне CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: Template:$na SDW-CPET-ENC EncryptionError: Template:vC
SDW-CPET-SCR	Scripts	Изменение скриптов в шаблоне CPE	info	low	При нажатии: Save, Run	Standard/Extended: Code Event: Username:$us Template:$name, Owner:$owner, OrcVersion:$o Changed: $SriptName] SDW-CPET-SCR Scripts: Username:admin(tena Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am custom_config]
SDW-CPET-SCR	ScriptsError	Изменение скриптов в шаблоне CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: CPE:$name, T $ErrorMessage SDW-CPET-SCR ScriptsError: Template:vCPE1,

SDW-CPET-NET	Interface	Добавление/ Удаление/ Изменение зоны/IP адреса/ MAC адреса/QoS интерфейса в шаблоне CPE	info	low	При нажатии: Save	Standard: Code Event: Username:$username($t Owner:$owner, OrcVersion:$orcversion, Alias:$a SDW-CPET-NET Interface: Username:admin(ter Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am SDW-CPET-NET Interface: Username:admin(ter Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am SDW-CPET-NET Interface: Username:admin(ter Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am Extended: Code Event: Username:$username($ Owner:$owner, OrcVersion:$orcversion, Alias: $a QOS: $Detailed_change] SDW-CPET-NET Interface: Username:admin(ter Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am Bridge:false, Enable automatically:true, IPv4 inpu netmask:255.0.0.0, IPv4 gateway:10.1.1.254, IPv4 b MAC:01:01:01:01:01:01, Generate MAC:true, Adde BE(MinR):10, BE(MaxR):100] SDW-CPET-NET Interface: Username:admin(ter Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am Bridge:false, Enable automatically:true, IPv4 inpu netmask:255.0.0.0, IPv4 gateway:10.1.1.254, IPv4 b MAC:01:01:01:01:01:01, Generate MAC:true, Delet MaxRate:1000, BE(MinR):10, BE(MaxR):100] SDW-CPET-NET Interface: Username:admin(ter Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.am lan>lan(tenant-1), Bridge:false>true, Enable auto Manually>From IP pool, IPv4 address: 10.1.1.1>10.2.2 IPv4 gateway: 10.1.1.254>10.2.2.254, IPv4 broadcas 01:01:01:01:01:01>02:02:02:02:02:02, Generate MA QoS:true, MaxRate:100, BE(MinR):20, BE(MaxR):9 Показываем изменение с/на при Change в GE Не отображается изменение с/на при Change параметры.
SDW-CPET-NET	InterfaceError	Добавление/ Удаление/ Изменение зоны/IP адреса/ MAC адреса/QoS интерфейса в шаблоне CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: Template:$na QoS], $ErrorMessage SDW-CPE-NET InterfaceError: Template:vCPE1 lan, [GEN], $ErrorMessage SDW-CPE-NET InterfaceError: Template:vCPE1 lan, [QoS], $ErrorMessage
SDW-CPET-STR	StaticRoute	Добавление/ Удаление/ Изменение настроек статических маршрутов в шаблоне CPE	info	low	При нажатии: Save	Standard/Extended: Code Event: Username:$us Template:$name, Owner:$owner, OrcVersion:$o VRF:$vrf, Destination:$destination/$ipv4netma Gateway:$gateway, Interface:$interface, Metric Type:$type] SDW-CPET-STR StaticRoute: Username:admin(Template:vCPE1, Owner:tenant-1, OrcVersion:3.0 VRF:main/254, Destination:10.1.1.1/255.0.0.0, Gate MTU:1500, AD:20, Type:unicast] SDW-CPET-STR StaticRoute: Username:admin(Template:vCPE1, Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.amd64, [Deleted: V Gateway:10.1.1.254, Interface:lan, Metric:20, MTU: SDW-CPET-STR StaticRoute: Username:admin(Template:vCPE1, Owner:tenant-1, OrcVersion:3.0 VRF:yellow/100, Destination:10.2.2.2/255.255.0.0 Metric:10, MTU:1300, AD:10, Type:blackhole] Не отображается изменение с/на при Change параметры.
SDW-CPET-STR	StaticRouteError	Изменение настроек статических маршрутов в шаблоне CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: Template:$na SDW-CPE-STR StaticRoute: Template:vCPE1, C

Управление конфигурацией шаблона межсетевого экрана (Firewall template configuration management)						
SDW-FWT	Firewall	Создание/ Удаление/ Изменение правил шаблона МЭ	info	low	При нажатии: Save	При создании/удалении шаблона: Standard/Extended: Code Event: Username:$us Name:$name, Owner:$owner, OrcVersion:$orcv SDW-FWT Firewall: Username:admin(tenant-1), template, Owner:admin(tenant-1), OrcVersion:3. SDW-FWT Firewall: Username:admin(tenant-1), template, Owner:admin(tenant-1), OrcVersion:3. При изменении: Standard: Code Event: Username:$username($t Owner:$owner, OrcVersion:$orcversion, [Chang SDW-FWT Firewall: Username:admin(tenant-1), template, Owner:admin(tenant-1), OrcVersion:3. Extended: Code Event: Username:$username($ Owner:$owner, OrcVersion:$orcversion, [Added || NAT || ZF || IPSET || DPI: $Detailed_change] SDW-FWT Firewall: Username:admin(tenant-1), template, Owner:admin(tenant-1), OrcVersion:3. Syn-flood protection:Disable, Default INPUT act SDW-FWT Firewall: Username:admin(tenant-1), template, Owner:admin(tenant-1), OrcVersion:3. (Name:Test, Action:ACCEPT, IPset:null, IPv:IPv4, DstIP:3.3.3.3:4.4.4.4, Proto:icmp, + new rule), Dele IPset:null, IPv:IPv4, SrcZ:wan, DstZ: lan, SrcIP:11.11.1 rule), Changed: RUL: (Name:Allow-Ping, Action:D DstZ:null, SrcIP:null, DstIP:null, Proto:icmp, + new SDW-FWT Firewall: Username:admin(tenant-1), template, Owner:admin(tenant-1), OrcVersion:3. (Status:On, Name:Test, Ptags:null, Table:FILTER, Placement:Pre-rules,Start of table, DstIP:1.1.1.1, M Target:ACCEPT, Frag:false, MarkVal:null, MarkMa StrSrchPatt:null, StrAlg:BM, StrRange:1-65535, S RecentName:null, RecentProto:SET, RecentSec: applet,WebAsm, ..., + new rule), Deleted: ADVR: (Changed: ADVR: (Status:Off, Name:ICMP ..., + ne SDW-FWT Firewall: Username:admin(tenant-1), template, Owner: admin(tenant-1), OrcVersion:3 NAT:DNAT: (Name:Test, Proto:IP, SP-DestIP:1.1.1.1, SrcIP:11.1.1.1,TP-DstIP:192.1.1.1, TP-DestZone:wan(te (Name:Test, Proto:IP, SP-DestIP:1.1.1.1, SP-SrcZon DstIP:192.1.1.1, TP-DestZone:wan(tenant-1), + new Proto:IP, SP-DestIP:1.1.1.1, SP-SrcZone:lan(tenant DestZone:wan(tenant-1), + new rule)] SDW-FWT Firewall: Username:admin(tenant-1), template, Owner: admin(tenant-1), OrcVersion:3 (From:Any zone, To:mgmt,+ new rule), Deleted: Z Changed: ZF: (From:wan, To:lan,+ new rule)] SDW-FWT Firewall: Username:admin(tenant-1), template, Owner: admin(tenant-1), OrcVersion:3 (Name:test, Direction:Match source, Type:Set o 254]/24,20.2.2.[1-5], + new rule), Deleted: IPSET: Type:Set of subnets, EntryList:10.1.1.[1-254]/24,2 (Name:test, Direction:Match source, Type:Set o 254]/24,20.2.2.[1-5], + new rule)] SDW-FWT Firewall: Username:admin(tenant-1), template, Owner:admin(tenant-1), OrcVersion:3. PKTmark:1,2,3,4] PKTmark: отображаются только включенные, и Не отображается изменение с/на при Change параметры.
SDW-FWT	FirewallError	Создание/ Удаление/ Изменение правил шаблона МЭ с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: Name:$name, NAT, ZF || IPSET || DPI], $ErrorMessage SDW-FWT FirewallError: Name:Default firewall t ADVR || NAT, ZF || IPSET || DPI], $ErrorMessage

Управление зонами межсетевого экрана (Firewall zones configuration management)						
SDW-FWZ	Zone	Создание/ Удаление/ Изменение правил зон шаблона МЭ	info	low	При нажатии: Save	Standard: Code Event: Username:$username($t Owner:$owner, OrcVersion:$orcversion, [Added SDW-FWZ Zone: Username:admin(tenant-1), Us Owner:admin(tenant-1), OrcVersion:3.0.0.release Changed] Extended: Code Event: Username:$username($ Owner:$owner, OrcVersion:3.0.0.release.1.cis.am $Detailed_change] SDW-FWZ Zone: Username:admin(tenant-1), Us Owner:admin(tenant-1), OrcVersion:3.0.0.release Output:ACCEPT, Forwarding:ACCEPT, Masquer Drop logging:false, Networks:11.1.1.1/32, 22.2.2.2/32 SDW-FWZ Zone: Username:admin(tenant-1), Us Owner:admin(tenant-1), OrcVersion:3.0.0.release Output:ACCEPT, Forwarding:ACCEPT, Masquer Drop logging:false, Networks:11.1.1.1/32, 22.2.2.2/32 SDW-FWZ Zone: Username:admin(tenant-1), Us Owner:admin(tenant-1), OrcVersion:3.0.0.release Output:ACCEPT, Forwarding:REJECT, Masquera Drop logging:false, Networks:11.1.1.1/32, 33.3.3.3/3 Не отображается изменение с/на при Change параметры.
SDW-FWZ	ZoneError	Создание/ Удаление/ Изменение правил зон шаблона МЭ с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: Name:$name, SDW-FWT ZoneError: Name:lan, Owner:tenant-
Загрузка прошивки (Upload firmware)						
SDW-FMW	Firmware	Загружена прошивка, проверка целостности пакета.	info	info	При нажатии: +Firmware	Standard/Extended: Code Event: Username:$us [Added || Deleted: $FwName] SDW-FMW Firmware: Username:admin(tenant-1 knaas-cpe_2.25.09.release.21.bios.amd64-vkesr-
SDW-FMW	FirmwareError	Загружена прошивка, проверка целостности пакета с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: $ErrorMessag SDW-FWT FirmwareError: $ErrorMessage
Запланированные события (Scheduled events)						
SCH-FMWU	FirmwareUpdate	Обновление прошивки на CPE	info	low	При получении подтверждения от CPE, что обновление успешно	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name, [SDW-FMWU FirmwareUpdate: Username:admin Template:vCPE1, CTenant:tenant-1, [Update: kna vkesr-m1_en-US_ru-RU.tar>knaas-cpe_2.25.09.r US_ru-RU.tar]
SCH-FMWU	FirmwareUpdateError	Обновление прошивки на CPE	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: Username:$us CPE:$name, Template:$name, CTenant:$name, $ SDW-FMWU FirmwareUpdate: Username:admin Template:vCPE1, CTenant:tenant-1, $ErrorMessa
SCH-UPDS	UpdateSettings	Запланированное изменение конфигурации CPE	info	low	В момент наступления времени выполнения	Standard/Extended: Code Event: Username:$us [Scheduled: CPE:$name, Time:$time] SCH-UPDS UpdateSettings: Username:admin(te CPE:vCPE1, Time:$time]
SCH-UPDS	UpdateSettingsError	Запланированное изменение конфигурации CPE с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: $ErrorMessag SCH-UPDS UpdateSettingsError: $ErrorMessag
Идентификация и аутентификация пользователей (User identification and authentication)						

USR-USR	Authentication	Аутентификация на оркестратор успешное	info	low	В момент подключения пользователя	Standard/Extended: Code Event: Username:$us Role:$role, Account type:$type, Group:$group, Permissions:$permissions, PermissionsID:$id, Au USR-USR Authentication: Username:admin(tena Account type:LDAP, Group:admin, Permissions:F d82e-4dfb-b7bc-414cca14abc5, Authentication
USR-USR	AuthenticationError	Аутентификация на оркестратор с ошибкой	warn	medium	Сразу при возникновении	Standard/Extended: Code Event: Username:$us Role:$role, Account type:$type, Group:$group, F PermissionsID:$id, Authentication by password \| USR-USR AuthenticationError: Username:admin Account type:LDAP, Group:admin, Permissions:F d82e-4dfb-b7bc-414cca14abc5, Authentication Если пользователя не существует то: Standard/Extended: Code Event: Username:$us by password, $ErrorMessage USR-USR AuthenticationError: Username:admin password, $ErrorMessage
USR-USR	UserChange	Создание/ Удаление/ Изменение ролей, разрешений, 2FA, пароля, пользователя.	info	low	При нажатии: Save	Standard: Code Event: Username:$username($t || Changed || Blocked || Unblocked || Password ch USR-USR UserChange: Username:admin(tenant USR-USR UserChange: Username:admin(tenant USR-USR UserChange: Username:admin(tenant UserTenant1] USR-USR UserChange: Username:admin(tenant USR-USR UserChange: Username:admin(tenant UserTenant1] USR-USR UserChange: Username:admin(tenant UserTenant1] USR-USR UserChange: Username:admin(tenant UserTenant1] Extended: Code Event: Username:$username($ || Changed || Blocked || Unblocked || Password ch $Detailed_change] USR-USR UserChange: Username:admin(tenant $name, Account type:Local, Login:UserTenant1, 2FA:false, Request confirmation is required:false Email:boris.britva@snatch.com] USR-USR UserChange: Username:admin(tenant $name, Account type:Local, Login:UserTenant1, 2FA:false, Request confirmation is required:false Email:boris.britva@snatch.com] USR-USR UserChange: Username:admin(tenant $name, Account type:Local, Login:UserTenant1, 2FA:false, Request confirmation is required:false Email:boris.britva@snatch.com]

USR-PERM	UserPermissions	Создание/ Удаление/ Изменение прав доступа.	info	low	При нажатии: Save	Standard: Code Event: Username:$username($t || Changed: $PermissionsName] USR-PERM UserPermissions: Username:admin(t access] USR-PERM UserPermissions: Username:admin(t access] USR-PERM UserPermissions: Username:admin(t access] Extended: Code Event: Username:$username($ || Changed: $PermissionsName, $Detailed_chan USR-PERM UserPermissions: Username:admin(t All:Editing || Viewing || No access, Infrastructure: Domain:Editing || Viewing || No access, Data cent VIM:Editing || Viewing || No access, Controller:Ed USR-PERM UserPermissions: Username:admin(t All:Editing || Viewing || No access, Infrastructure: Domain:Editing || Viewing || No access, Data cent VIM:Editing || Viewing || No access, Controller:Ed USR-PERM UserPermissions: Username:admin(t $name, All:Editing || Viewing || No access, Infrast Domain:Editing || Viewing || No access, Data cent VIM:Editing || Viewing || No access, Controller:Ed
Взаимодействие с внешними СЗИ: IDS/AV/DLP (Interaction with external information security systems: IDS/AV/D						
SYS-API	Call	Совершен вызов метода API	info	low	В момент исполнения	Standard/Extended: Code Event API-[$API_pa Username:$username($tenant), srclp:$srclp, Ob метод API] SYS-API Call: API-[/api/nfv/sdwan/cpe/invento 1), Userlp:127.0.0.1, Obj:[..]
SYS-API	CallComplete	Завершен вызов метода API	info	low	В момент исполнения	Standard/Extended: Code Event API-[$API_pa DELETE]: Username:$username($tenant), srclp: вызывается метод API], Ret: [код возврата] SYS-API CallComplete: API-[/api/nfv/sdwan/cp [GET]: Username:admin(tenant-1), Userlp:127.0.0.

Ниже представлен список событий безопасности, которые регистрируются в журнале аудита на устройствах CPE.

Таблица 2. Перечень событий безопасности, регистрируемых на устройствах CPE

Уровень устройства . серьезности (Код) / Facility.Severity (Code)	Служба / Application	Имя события / Event	Действие	Уровень Severity события Kuma	Момент активации	Пример отображаемого события в журнале / Message
Идентификация и аутентификация пользователей (User identification and authentication)						
authpriv.info (10.6)	dropbear	Child connection from	Аутентификация на устройство	low	В момент исполнения	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	Max auth tries reached	Аутентификация на устройство	high	В момент исполнения	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	Password auth succeeded	Аутентификация на устройство	low	В момент исполнения	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	Bad password attempt	Аутентификация на устройство	medium	В момент исполнения	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
Управление конфигурацией МЭ/CPE (Firewall/CPE Configuration Management)						
user.info (1.6)	sdwan-oob	Recieved and execute task firewall	Изменение правил МЭ	low	В момент исполнения	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 stopped	Остановка сервиса МЭ	critical	В момент исполнения	Thu Oct 23 13:04:40 2025 user.crit firewall: Firewall stopped
user.info (1.6)	firewall	Firewall started	Запуск сервиса МЭ	low	В момент исполнения	Thu Oct 23 13:04:44 2025 user.info firewall: Firewall started
user.warn (1.4)	firewall	Firewall restarted	Перезапуск сервиса МЭ	medium	В момент исполнения	Thu Oct 23 13:04:55 2025 user.warn firewall: Firewall restarted
user.warn (1.4)	firewall	Firewall reloaded	Перезагрузка сервиса МЭ	medium	В момент исполнения	Thu Oct 23 13:04:59 2025 user.warn firewall: Firewall reloaded
Логирование фильтрации/передачи трафика на МЭ (Logging of traffic filtering/transmission on the firewall)						
kern.info (0.6)	kernel	FW-AUD	Аудит работы МЭ	low	В момент исполнения	Sat Nov 1 11:54:41 2025 kern.info kernel: [337220.6950 FW-AUD= OUT=eth0 SRC=172.17.9.221 DST=172.17.9.203 LEN=299 TOS=0x00 PREC=0xC0 TTL=64 ID=39548 D PROTO=TCP SPT=54280 DPT=6653 WINDOW=3219 RES=0x00 ACK PSH URGP=0 MARK=0x1f4
Проверка целостности МЭ/CPE (Firewall/CPE Integrity Check)						
user.info (1.6)	sdwan	Integrity check successful	Контроль целостности не нарушен	low	В момент исполнения	Thu Apr 9 11:45:44 2026 user.info sdwan[31284]: Integ check successful
user.crit (1.2)	sdwan	Integrity check failed	Нарушение контроля целостности файлов	critical	В момент исполнения	Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]: Integ check failed
user.crit (1.2)	sdwan	Verification mismatch with 'Gost2012' checker. Reason: File <$file>	Нарушение контроля целостности файлов	critical	В момент исполнения	Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]: Verification mismatch with 'Gost2012' checker. Reaso File "/usr/sbin/sdwan" has unexpected hash Vmd5sJ2GwLK35woBdeivZ1NAtsXlZNDBga2W4LH5 != expected ttDJAQ1XW+UmYx4RdVru2YFWR2Al1YzG9BO4Nvx2
user.crit (1.2)	sdwan	Integrity check failed. Traffic forwarding blocked	Блокировка трафика	critical	В момент исполнения	Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]: Integ check failed. Traffic forwarding blocked
user.info (1.6)	sdwan	Firewall self-test successful	Успешная проверка МЭ	info	В момент исполнения	Thu Feb 26 12:15:48 2026 user.info sdwan[7241]: Successful firewall self test
user.crit (1.2)	sdwan	Firewall self-test failed	Неуспешная проверка МЭ	critical	В момент исполнения	Thu Feb 26 13:27:06 2026 user.crit sdwan[30591]: Fire self test failed
Подключение USB устройств (Connecting USB devices)						
kern.info (0.6)	kernel	usb	Подключение USB устройства	medium	В момент исполнения	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	Монтирование USB устройства	high	В момент исполнения	Tue Feb 10 08:09:30 2026 kern.info kernel: [191.87720 EXT4-fs (sdb2): mounted filesystem with ordered dat mode. Opts: (null)
Изменение времени (Time change)						
daemon.warn (3.4)	chronyd	time jump detected	Изменение времени	medium	В момент исполнения	Tue Feb 10 08:04:13 2026 daemon.warn chronyd[4428 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[835 Can't synchronise: no selectable sources Tue Feb 10 08:58:33 2026 daemon.info chronyd[835 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

Диапазоны IP-адресов и подсетей для устройств CPE

Вы можете создавать диапазоны IP-адресов и подсетей для централизованного назначения IPv4-адресов при создании или изменении сетевых интерфейсов устройств CPE. Диапазоны IP-адресов также можно использовать для централизованного назначения IPv4-адресов идентификаторам маршрутизатора устройств CPE при настройке основных параметров BGP.

Работа с диапазонами IP-адресов

Для просмотра таблицы диапазонов IP-адресов вам нужно в меню перейти в раздел **SD-WAN → IPAM**. По умолчанию выбрана вкладка **Диапазоны IP**. Информация о диапазонах IP-адресов отображается в следующих столбцах таблицы:

- **Имя** – имя диапазона IP-адресов.
- **CIDR** – IPv4-префикс подсети, в которой находится диапазон IP-адресов.
- **Диапазон IP** – начальное и конечное значения диапазона IP-адресов.
- **Использование** – количество IP-адресов в диапазоне, которые были назначены сетевым интерфейсам или идентификаторам маршрутизатора устройств CPE.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание диапазона IP-адресов

Чтобы создать диапазон IP-адресов:

1. В меню перейдите в раздел **SD-WAN → IPAM**.

   По умолчанию выбрана вкладка **Диапазоны IP**, на которой отображается таблица диапазонов IP-адресов.

2. В верхней части страницы нажмите на кнопку **+ Диапазон IP**.
3. В открывшемся окне в поле **Имя** введите имя диапазона IP-адресов. Максимальная длина имени: 32 символа.
4. В поле **CIDR** введите IPv4-префикс подсети, в которой находится диапазон IP-адресов.

5. Укажите диапазон IP-адресов. Для этого в блоке **Диапазон IP** нажмите на кнопку **+ Добавить**, после чего введите начальное и конечное значения диапазона IP-адресов.

   Диапазон IP-адресов будет указан и отобразится в блоке **Диапазон IP**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазоны IP-адресов. Для удаления диапазона IP-адресов нажмите рядом с ним на значок удаления ✕.

6. Нажмите на кнопку **Создать**.

Диапазон IP-адресов будет создан и отобразится в таблице.

Изменение диапазона IP-адресов

Чтобы изменить диапазон IP-адресов:

1. В меню перейдите в раздел **SD-WAN → IPAM**.

   По умолчанию выбрана вкладка **Диапазоны IP**, на которой отображается таблица диапазонов IP-адресов.

2. Нажмите на диапазон IP-адресов, который вы хотите изменить.

3. В открывшемся окне при необходимости измените имя и IPv4-префикс подсети, в которой находится диапазон IP-адресов, а также укажите или удалите диапазоны IP-адресов.

4. В верхней части области настройки нажмите на кнопку **Сохранить**.

Диапазон IP-адресов будет изменен и обновится в таблице.

Просмотр использования диапазона IP-адресов

При необходимости вы можете посмотреть, какие шаблоны CPE и устройства CPE используют диапазон IP-адресов. Например, если диапазон IP-адресов используется, его невозможно удалить. Вы также можете посмотреть информацию об IP-адресах, которые были назначены из диапазона IP-адресов.

Чтобы посмотреть, используется ли диапазон IP-адресов:

1. В меню перейдите в раздел **SD-WAN → IPAM**.

   По умолчанию выбрана вкладка **Диапазоны IP**, на которой отображается таблица диапазонов IP-адресов.

2. Нажмите на диапазон IP-адресов, использование которого вы хотите посмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона IP-адресов.

3. Посмотрите использование диапазона IP-адресов одним из следующих способов:

   - Если вы хотите посмотреть, какие устройства CPE используют диапазон IP-адресов, выберите вкладку **Использование** → **CPE**.

     Отобразится список устройств CPE, использующих диапазон IP-адресов.

   - Если вы хотите посмотреть, какие шаблоны CPE используют диапазон IP-адресов, выберите вкладку **Использование** → **Шаблон**.

     Отобразится список шаблонов CPE, использующих диапазон IP-адресов.

4. Если вы хотите посмотреть информацию об IP-адресах, которые были назначены из диапазона IP-адресов, выберите вкладку **Аренды**.

   Отобразится таблица IP-адресов, назначенных из диапазона IP-адресов. Информация об IP-адресах отображается в следующих столбцах таблицы:

   - **IP** – IP-адрес, который был назначен из диапазона IP-адресов.
   - **CPE** – устройство CPE, которому был назначен IP-адрес.
   - **Тип** – информация о том, был ли IP-адрес назначен сетевому интерфейсу или идентификатору маршрутизатора устройства CPE.
   - **Имя** – имя сетевого интерфейса, которому был назначен IP-адрес. Если IP-адрес был назначен идентификатору маршрутизатора устройства CPE, значение в этом столбце не отображается.
   - **Тенант** – тенант, которому добавлено устройство CPE.

Действия, которые вы можете выполнить со списками и таблицей, описаны в инструкции Работа с таблицами компонентов решения.

Удаление диапазонов IP-адресов

Невозможно удалить диапазон IP-адресов, если он используется хотя бы одним шаблоном CPE или устройством CPE. Для удаления диапазона IP-адресов, который используется шаблонами CPE или устройствами CPE, вам нужно сначала убрать диапазон IP-адресов из параметров сетевых интерфейсов и параметров протокола BGP. Вы можете посмотреть, какие шаблоны CPE и устройства CPE используют диапазон IP-адресов.

Удаленные диапазоны IP-адресов невозможно восстановить.

Чтобы удалить диапазоны IP-адресов:

1. В меню перейдите в раздел **SD-WAN → IPAM**.

   По умолчанию выбрана вкладка **Диапазоны IP**, на которой отображается таблица диапазонов IP-адресов.

2. Если вы хотите удалить отдельный диапазон IP-адресов, выполните следующие действия:

   a. Нажмите на диапазон IP-адресов, который вы хотите удалить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона IP-адресов.

   b. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

3. Если вы хотите удалить несколько диапазонов IP-адресов, выполните следующие действия:

   a. Установите флажки рядом с диапазонами IP-адресов, которые вы хотите удалить.

   b. В верхней части таблицы нажмите на кнопку **Действия → Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Диапазоны IP-адресов будут удалены и перестанут отображаться в таблице.

Работа с диапазонами подсетей

Для просмотра таблицы диапазонов подсетей вам нужно в меню перейти в раздел **SD-WAN → IPAM** и выбрать вкладку **Диапазоны подсетей**. Информация о диапазонах подсетей отображается в следующих столбцах таблицы:

- **Имя** – имя диапазона подсетей.
- **CIDR** – IPv4-префикс диапазона подсетей.
- **Использование** – количество подсетей, которые были назначены сетевым интерфейсам.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание диапазона подсетей

Чтобы создать диапазон подсетей:

1. В меню перейдите в раздел **SD-WAN → IPAM**.

   По умолчанию выбрана вкладка **Диапазоны IP**, на которой отображается таблица диапазонов IP-адресов.

2. Выберите вкладку **Диапазоны подсетей**.

   Отобразится таблица диапазонов подсетей.

3. В верхней части страницы нажмите на кнопку **+ Диапазон подсетей**.
4. В открывшемся окне в поле **Имя** введите имя диапазона подсетей. Максимальная длина имени: 32 символа.
5. В поле **Базовый CIDR** введите IPv4-префикс диапазона подсетей.
6. В поле **Суб-префикс** введите длину IPv4-префикса подсетей в диапазоне подсетей. Диапазон значений: от 0 до 32.
7. Нажмите на кнопку **Создать**.

Диапазон подсетей будет создан и отобразится в таблице.

Изменение диапазона подсетей

Чтобы изменить диапазон подсетей:

1. В меню перейдите в раздел **SD-WAN → IPAM**.

   По умолчанию выбрана вкладка **Диапазоны IP**, на которой отображается таблица диапазонов IP-адресов.
2. Выберите вкладку **Диапазоны подсетей**.

   Отобразится таблица диапазонов подсетей.
3. Нажмите на диапазон подсетей, который вы хотите изменить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона подсетей.
4. В открывшемся окне при необходимости измените следующие параметры:
   - имя диапазона подсетей;
   - IPv4-префикс диапазона подсетей;
   - длину IPv4-префикса подсетей в диапазоне подсетей.
5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры диапазона подсетей.

Диапазон подсетей будет изменен и обновится в таблице.

Просмотр использования диапазона подсетей

При необходимости вы можете посмотреть, какие шаблоны CPE и устройства CPE используют диапазон подсетей. Например, если диапазон подсетей используется, его невозможно удалить. Вы также можете посмотреть информацию о подсетях, которые были назначены из диапазона подсетей.

Чтобы посмотреть, используется ли диапазон подсетей:

1. В меню перейдите в раздел **SD-WAN → IPAM**.

   По умолчанию выбрана вкладка **Диапазоны IP**, на которой отображается таблица диапазонов IP-адресов.

2. Выберите вкладку **Диапазоны подсетей**.

   Отобразится таблица диапазонов подсетей.

3. Нажмите на диапазон подсетей, использование которого вы хотите посмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона подсетей.

4. Посмотрите использование диапазона подсетей одним из следующих способов:

   - Если вы хотите посмотреть, какие устройства CPE используют диапазон подсетей, выберите вкладку **Использование → CPE**.

     Отобразится список устройств CPE, использующих диапазон подсетей.

   - Если вы хотите посмотреть, какие шаблоны CPE используют диапазон подсетей, выберите вкладку **Использование → Шаблон**.

     Отобразится список шаблонов CPE, использующих диапазон подсетей.

5. Если вы хотите посмотреть информацию о подсетях, которые были назначены из диапазона подсетей, выберите вкладку **Аренды**.

   Отобразится таблица подсетей, назначенных из диапазона подсетей. Информация о подсетях отображается в следующих столбцах таблицы:

   - **CIDR** – IPv4-префикс подсети, которая была назначена из диапазона подсетей.
   - **CPE** – устройство CPE, которому был назначен IPv4-адрес из подсети.
   - **Имя** – имя сетевого интерфейса, которому был назначен IPv4-адрес из подсети.
   - **Тенант** – тенант, которому было добавлено устройство CPE.

Действия, которые вы можете выполнить со списками и таблицей, описаны в инструкции Работа с таблицами компонентов решения.

Удаление диапазонов подсетей

Невозможно удалить диапазон подсетей, если он используется хотя бы одним шаблоном CPE или устройством CPE. Для удаления диапазона подсетей, который используется шаблонами CPE или устройствами CPE, вам нужно сначала убрать диапазон подсетей из параметров сетевых интерфейсов и параметров протокола BGP. Вы можете посмотреть, какие шаблоны CPE и устройства CPE используют диапазон подсетей.

Удаленные диапазоны подсетей невозможно восстановить.

Чтобы удалить диапазоны подсетей:

1. В меню перейдите в раздел **SD-WAN → IPAM**.

   По умолчанию выбрана вкладка **Диапазоны IP**, на которой отображается таблица диапазонов IP-адресов.

2. Выберите вкладку **Диапазоны подсетей**.

   Отобразится таблица диапазонов подсетей.

3. Если вы хотите удалить отдельный диапазон подсетей, выполните следующие действия:

   a. Нажмите на диапазон подсетей, который вы хотите удалить.

      В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона подсетей.

   b. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. Если вы хотите удалить несколько диапазонов подсетей, выполните следующие действия:

   a. Установите флажки рядом с диапазонами подсетей, которые вы хотите удалить.

   b. В верхней части таблицы нажмите на кнопку **Действия → Удалить**.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Диапазоны подсетей будут удалены и перестанут отображаться в таблице.

Управление межсетевым экраном

Существует два основных подхода к фильтрации трафика:

- классический фильтр сетевого трафика
- межсетевой экран, ориентированный на зоны

Модель фильтра сетевого трафика предлагает низкий уровень абстракции: правила определяют поведение каждого отдельного пакета. В синтаксисе пакетного фильтра, такого как iptables, *правила* привязываются к *цепочкам*, которые формируются в *таблицы*. Каждый пакет проходит через несколько таблиц, а в каждой таблице – через одну из стандартных цепочек. Принадлежность правил таблицам (filter, nat, mangle, raw и т.д.) осуществляется обычно по типу выполняемых действий. Правила часто привязываются к конкретным интерфейсам (входящим и исходящим). Чтобы охватить несколько дополнительных интерфейсов, правила необходимо копировать и модифицировать.

Модель межсетевого экрана, ориентированного на зоны, предлагает высокий уровень абстракции: зоны являются контейнерами для интерфейсов, а политика (набор правил) определяет взаимодействие между зонами.

Зоны (Zone) – логические группы интерфейсов, которые считаются однотипными с точки зрения политики безопасности.

Политика (набор правил) определяется между зонами. Правила пишутся один раз для пары зон (Zone A ↔ Zone B) и автоматически применяются ко всем интерфейсам, принадлежащим этим зонам. Трафик классифицируется по протоколу, адресу и сопоставляется с политикой между двумя зонами.

Таким образом, концепция **межсетевого экрана, ориентированного на зоны**, совпадает с таблицами и цепочками **пакетного фильтра** типа iptables лишь на уровне низкоуровневой обработки пакетов. К пакетному фильтру она добавляет логическую группировку и централизованную политику, что делает администрирование более масштабируемым, менее подверженным ошибкам и упрощает повторное использование.

В Kaspersky SD-WAN реализованы оба описанных выше подхода к фильтрации пакетов трафика на устройствах CPE.

Межсетевой экран может принимать (англ. accept), отбрасывать (англ. drop) и отклонять (англ. reject) пакеты трафика. При отклонении пакета трафика его отправитель получает сообщение `icmp-reject`. Каждое из действий межсетевой экран может применять ко входящим и исходящим пакетам трафика, а также к пакетам трафика, пересылаемыми между сетевыми интерфейсами и подсетями устройств CPE. При настройке основных параметров межсетевого экрана требуется указать действия по умолчанию, которые межсетевой экран выполняет с пакетами трафика.

Для централизованной настройки межсетевого экрана устройств CPE используются шаблоны межсетевого экрана. Вы можете указать необходимые параметры фильтрации в шаблоне межсетевого экрана, после чего указать этот шаблон межсетевого экрана при добавлении или ручной регистрации устройств CPE, чтобы не настраивать параметры на каждом отдельном устройстве CPE. Если вы измените параметр в шаблоне межсетевого экрана, параметр автоматически изменится на всех устройствах CPE, которые используют шаблон межсетевого экрана. Если вы измените параметр на устройстве CPE, параметр перестанет зависеть от шаблона межсетевого экрана и при изменении в шаблоне межсетевого экрана не будет изменяться на устройстве CPE.

Зоны межсетевого экрана

Вы можете добавить сетевые интерфейсы и подсети в зону межсетевого экрана (англ. firewall zone, далее также зона), чтобы принимать, отбрасывать или отклонять пакеты трафика, передающиеся через сетевые интерфейсы и подсети. Когда вы создаете или изменяете зону межсетевого экрана, вам нужно указать действия, которые выполняются с паами трафика, а также при необходимости добавить подсети. Вы можете добавить сетевые интерфейсы в зону межсетевого экрана при создании или изменении сетевых интерфейсов.

Если вы хотите разрешить передачу пакетов трафика из одной зоны межсетевого экрана в другую, вам нужно создать передачу (англ. forwarding). При создании передачи требуется указать исходящую и входящую зоны межсетевого экрана.

Поддерживается создание общих зон межсетевого экрана, которые могут использовать несколько устройств CPE, а также зон межсетевого экрана на отдельном устройстве CPE.

Стандартные правила межсетевого экрана (межсетевой экран, ориентированный на зоны)

Вы можете создавать стандартные правила межсетевого экрана, чтобы принимать, отбрасывать или отклонять пакеты трафика на основании указанных критериев. Например, вы можете создать правило межсетевого экрана, которое отклоняет пакеты трафика с указанной зоной межсетевого экрана источника.

Если вы хотите указать в параметрах нескольких правил межсетевого экрана одинаковые IP-адреса или подсети, вы можете создать набор IP (англ. IP set). При создании набора IP требуется указать, относятся ли IP-адреса или подсети к источнику или назначению. Вы можете указать созданный набор IP при создании или изменении правила межсетевого экрана.

Когда пакет трафика передается на устройство CPE, с пакетом трафика выполняется действие, указанное в параметрах одного из правил межсетевого экрана. Если ни одно из правил межсетевого экрана не может быть применено, с пакетом трафика выполняется действие, указанное в параметрах зоны межсетевого экрана, в которую пакет трафика был передан. Если пакет трафика не был передан ни в одну из зон межсетевого экрана, с пакетом трафика выполняется действие по умолчанию, которое вы указали при настройке основных параметров межсетевого экрана.

Расширенные правила межсетевого экрана (классический пакетный фильтр)

Расширенные правила межсетевого экрана предоставляют возможность более гибкой и гранулярной обработки пакетов по сравнению со стандартными правилами за счет использования дополнительных критериев соответствия и действий с пакетами. Вы можете использовать расширенные правила межсетевого экрана в ситуациях, когда использования стандартных правил недостаточно, например, когда требуется сопоставлять пакеты по дополнительным критериям или выполнить нестандартное целевое действие с пакетом. Так, если на CPE вы настроили несколько правил межсетевого экрана по зонам и интерфейсам, но вам нужно скрыть структуру сети, в которой находится CPE, вы можете создать дополнительное расширенное правило, которое будет отбрасывать пакеты с кодами ICMP, которые могут использоваться для изучения топологии сети, и поместить это расширенное правило на ранней стадии обработки трафика.

В соответствии с моделью классического пакетного фильтра, расширенные правила межсетевого экрана можно объединять в две группы. Первая позволяет добавлять новые правила перед существующими правилами (такие расширенные правила называются предправилами, англ. pre-rules) или во второй группе после существующих правил (такие расширенные правила называются постправилами, англ. post-rules). Порядок размещения правил определяет порядок обработки трафика. Наличие двух групп обработки правил в каждой цепочке каждой таблицы позволяет гибко менять логику обработки трафика отдельной группы правил, не нарушая логику и порядок обработки трафика в уже настроенной группе правил.

Правила межсетевого экрана, ориентированного на зоны, реализуются в классическом пакетном фильтре с помощью пользовательских (custom) цепочек. Поэтому стандартные правила, созданные на основе ориентированного на зоны подхода и расширенные правила, созданные в синтаксисе классического пакетного фильтра, не пересекаются и не взаимодействуют друг с другом.

Трансляция сетевых адресов

Межсетевой экран, ориентированный на зоны, поддерживает следующие механизмы трансляции сетевых адресов (англ. network address translation, NAT):

- DNAT-правила – могут заменять следующие компоненты пакетов трафика указанными значениями:
  - IP-адреса или префиксы назначения;
  - зоны межсетевого экрана назначения;
  - порты назначения (Port Address Translation, PAT).
- SNAT-правила – могут заменять IP-адреса или префиксы источника пакетов трафика указанными значениями.

DNAT-правила и SNAT-правила применяются к пакетам трафика на основании указанных критериев. Например, вы можете создать DNAT-правило, которое заменяет IP-адрес назначения пакетов трафика протокола TCP.

Трансляция сетевых адресов в синтаксисе классического пакетного фильтра описывается с помощью соответствующих действий в таблице mangle в расширенных правилах.

Работа с зонами межсетевого экрана

Вы можете посмотреть таблицу общих зон межсетевого экрана или таблицу зон межсетевого экрана на устройстве CPE:

- Для просмотра таблицы общих зон межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN** → **Зоны межсетевого экрана**.
- Для просмотра таблицы зон межсетевого экрана на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **CPE**, нажать на устройство CPE и выбрать вкладку **Межсетевой экран** → **Зоны**.

По умолчанию созданы следующие зоны межсетевого экрана:

- **wan** (WAN-зона межсетевого экрана) – зона межсетевого экрана для сетевых интерфейсов, которые подключены к WAN, например к интернету или сети оператора связи. В параметрах WAN-зоны межсетевого экрана включен маскарадинг, чтобы заменять IP-адрес источника исходящих из зоны межсетевого экрана пакетов трафика на IP-адрес, назначенный исходящему (англ. egress) сетевому интерфейсу.

- **lan** (LAN-зона межсетевого экрана) – зона межсетевого экрана для сетевых интерфейсов, которые подключены к LAN.

- **mgmt** (управляющая зона межсетевого экрана) – зона межсетевого экрана для сетевого интерфейса, который используется для пассивного мониторинга устройства CPE системой мониторинга Zabbix, а также для подключения оркестратора к устройству CPE по протоколу SSH.

Вы не можете удалить зоны межсетевого экрана по умолчанию или создать зоны межсетевого экрана с такими же именами.

Когда вы обновляете Kaspersky SD-WAN с версии 2.1 до 2.2, в параметрах всех шаблонов CPE происходят следующие изменения:

- в WAN-зону межсетевого экрана автоматически добавляются сетевые интерфейсы **sdwan<0–4>**;

- в LAN-зону межсетевого экрана автоматически добавляются сетевые интерфейсы **lan**, **br-lan** и **overlay**.

Информация об общих зонах межсетевого экрана отображается в следующих столбцах таблицы:

- **Имя** – имя зоны межсетевого экрана.

- **Использование** – использование зоны межсетевого экрана шаблонами межсетевого экрана, шаблонами CPE и устройствами CPE:

  - **Да**.

  - **Нет**.

- **Автор** – имя пользователя, который создал зону межсетевого экрана.

- **Создан** – дата и время создания зоны межсетевого экрана.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Информация о зонах межсетевого экрана на устройстве CPE отображается в следующих столбцах таблицы:

- **Имя** – имя зоны межсетевого экрана.

- **Параметры** – действия, которые межсетевой экран выполняет с пакетами трафика.

- **Сетевые интерфейсы/Сети** – сетевые интерфейсы и подсети, которые были добавлены в зону межсетевого экрана.

Создание зоны межсетевого экрана

Вы можете создать общую зону межсетевого экрана или зону межсетевого экрана на устройстве CPE.

Чтобы создать зону межсетевого экрана:

1. Перейдите к созданию зоны межсетевого экрана одним из следующих способов:

   - Если вы хотите создать общую зону межсетевого экрана, в меню перейдите в раздел **SD-WAN → Зоны межсетевого экрана** и в верхней части страницы нажмите на кнопку **+ Зона межсетевого экрана**.

   - Если вы хотите создать зону межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Зоны**, установите флажок **Переопределить** и нажмите на кнопку **+ Зона межсетевого экрана**.

   Отобразится таблица зон межсетевого экрана.

2. В открывшемся окне в поле **Имя** введите имя зоны межсетевого экрана. Максимальная длина имени: 255 символов.

3. В раскрывающемся списке **Вход** выберите действие, которое межсетевой экран выполняет со входящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Это значение выбрано по умолчанию.

   - **DROP** – отбрасывать пакеты трафика.

   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

4. В раскрывающемся списке **Выход** выберите действие, которое межсетевой экран выполняет с исходящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Это значение выбрано по умолчанию.

   - **DROP** – отбрасывать пакеты трафика.

   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

5. В раскрывающемся списке **Передача** выберите действие, которое межсетевой экран выполняет с пакетами трафика, пересылаемыми между сетевыми интерфейсами и подсетями:

   - **ACCEPT** – принимать пакеты трафика. Это значение выбрано по умолчанию.

   - **DROP** – отбрасывать пакеты трафика.

   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

6. Если вы хотите включить маскарадинг, чтобы заменять IP-адрес источника исходящих из зоны межсетевого экрана пакетов трафика на IP-адрес, назначенный исходящему (англ. egress) сетевому интерфейсу, выполните следующие действия:

   a. Установите флажок **Маскарадинг**. Этот флажок снят по умолчанию.

   b. Если вы хотите заменять IP-адрес источника только пакетов трафика с указанной подсетью источника, в блоке **Маскарадинг подсетей источника** нажмите на кнопку **+ Добавить** и введите IPv4-префикс подсети источника.

      Подсеть будет указана и отобразится в блоке **Маскарадинг подсетей источника**. Вы можете указать несколько подсетей и удалить подсети. Для удаления подсети нажмите рядом с ней на значок удаления ✕.

   c. Если вы хотите заменять IP-адрес источника только пакетов трафика с указанной подсетью назначения, в блоке **Маскарадинг подсетей назначения** нажмите на кнопку **+ Добавить** и введите IPv4-префикс подсети назначения.

      Подсеть будет указана и отобразится в блоке **Маскарадинг подсетей назначения**. Вы можете указать несколько подсетей и удалить подсети. Для удаления подсети нажмите рядом с ней на значок удаления ✕.

7. Если вы не хотите, чтобы межсетевой экран ограничивал значение MSS (Maximum Segment Size) передающихся через зону межсетевого экрана пакетов трафика до значения PMTU (Path Maximum Transmission Unit), после чего отнимал от него значение 40, снимите флажок **Ограничивать MSS до PMTU**. Значение 40 отнимается для исключения размера TCP-заголовка. Этот флажок установлен по умолчанию.

8. Если вы хотите, чтобы межсетевой экран вел журнал отброшенных в зоне межсетевого экрана пакетов трафика, установите флажок **Журналировать drop-ы**. Если созданные на устройстве CPE журналы отправляются на syslog-сервер, вы можете посмотреть журналы на syslog-сервере. Если созданные на устройстве CPE журналы хранятся локально, вы можете посмотреть журналы, запросив диагностическую информацию. Этот флажок снят по умолчанию.

9. Если сетевые интерфейсы подключены к коммутаторам или маршрутизаторам L3, и вы хотите передавать через зону межсетевого экрана пакеты трафика из подсетей коммутаторов или маршрутизаторов L3, добавьте в зону межсетевого экрана подсеть. Для этого в блоке **Сети** нажмите на кнопку **+ Добавить** и введите IPv4-префикс подсети.

   Подсеть будет добавлена и отобразится в блоке **Сети**. Вы можете добавить несколько подсетей и удалить подсети. Для удаления подсети нажмите рядом с ней на значок удаления ✕.

10. Нажмите на кнопку **Создать**.

    Зона межсетевого экрана будет создана и отобразится в таблице.

11. Если вы создали зону межсетевого экрана на устройстве CPE, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Вам нужно добавить в созданную зону межсетевого экрана сетевые интерфейсы. Это можно сделать при создании или изменении сетевого интерфейса. Если вы создали зону межсетевого экрана на устройстве CPE, вы можете добавить в зону межсетевого экрана только созданные на устройстве CPE сетевые интерфейсы.

Клонирование общей зоны межсетевого экрана

Вы можете клонировать созданную общую зону межсетевого экрана, чтобы создать такую же общую зону межсетевого экрана с другим именем. Клонирование зоны межсетевого экрана на устройстве CPE не поддерживается.

Чтобы клонировать общую зону межсетевого экрана:

1. В меню перейдите в раздел **SD-WAN → Зоны межсетевого экрана**.

   Отобразится таблица общих зон межсетевого экрана.

2. Нажмите на общую зону межсетевого экрана, которую вы хотите клонировать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Клонировать**.

4. В открывшемся окне введите имя новой общей зоны межсетевого экрана.

5. Нажмите на кнопку **Клонировать**.

Клон общей зоны межсетевого экрана с новым именем будет создан и отобразится в таблице.

Просмотр использования общей зоны межсетевого экрана

При необходимости вы можете посмотреть, какие шаблоны межсетевого экрана, а также шаблоны CPE и устройства CPE используют общую зону межсетевого экрана. Например, если общая зона межсетевого экрана используется, ее невозможно удалить.

Чтобы посмотреть, используется ли общая зона межсетевого экрана:

1. В меню перейдите в раздел **SD-WAN → Зоны межсетевого экрана**.

   Отобразится таблица общих зон межсетевого экрана.

2. Нажмите на общую зону межсетевого экрана, использование которой вы хотите посмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Показать использование**.

Откроется окно с таблицей шаблонов межсетевого экрана, шаблонов CPE и устройств CPE, использующих общую зону межсетевого экрана.

Изменение зоны межсетевого экрана

Вы можете изменить общую зону межсетевого экрана или зону межсетевого экрана на устройстве CPE.

Изменение общей зоны межсетевого экрана

Когда вы изменяете общую зону межсетевого экрана, новые параметры применяются ко всем устройствам CPE, которые используют общую зону межсетевого экрана. Это может привести к перегрузке оркестратора при наличии большого количества устройств CPE.

Чтобы изменить общую зону межсетевого экрана:

1. В меню перейдите в раздел **SD-WAN → Зоны межсетевого экрана**.

   Отобразится таблица общих зон межсетевого экрана.

2. Нажмите на общую зону межсетевого экрана, которую вы хотите изменить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

3. При необходимости измените параметры общей зоны межсетевого экрана. Описание параметров см. в инструкции по созданию зоны межсетевого экрана.

4. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры общей зоны межсетевого экрана.

   Откроется окно подтверждения с количеством устройств CPE, к которым будут применены новые параметры общей зоны межсетевого экрана.

5. Нажмите на кнопку **Да, изменить**.

Общая зона межсетевого экрана будет изменена и обновится в таблице.

Изменение зоны межсетевого экрана на устройстве CPE

Чтобы изменить зону межсетевого экрана на устройстве CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите изменить зону межсетевого экрана.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Межсетевой экран → Зоны**.

   Отобразится таблица зон межсетевого экрана.

4. Установите флажок **Переопределить**.

5. Нажмите на кнопку **Изменить** рядом с зоной межсетевого экрана, которую вы хотите изменить.

6. В открывшемся окне при необходимости измените параметры зоны межсетевого экрана. Описание параметров см. в инструкции по созданию зоны межсетевого экрана.

7. Нажмите на кнопку **Сохранить**.

   Зона межсетевого экрана будет изменена и обновится в таблице.

8. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Удаление зоны межсетевого экрана

Вы можете удалить общую зону межсетевого экрана или зону межсетевого экрана на устройстве CPE.

Удаленные зоны межсетевого экрана невозможно восстановить.

Удаление общей зоны межсетевого экрана

Вы не можете удалить общую зону межсетевого экрана, если она используется хотя бы одним шаблоном межсетевого экрана, шаблоном CPE или устройством CPE. Для удаления общей зоны межсетевого экрана, которая используется шаблонами межсетевого экрана, шаблонами CPE или устройствами CPE, вам нужно сначала убрать общую зону межсетевого экрана из их параметров. Вы можете посмотреть, какие шаблоны межсетевого экрана, шаблоны CPE и устройства CPE используют общую зону межсетевого экрана.

Чтобы удалить общую зону межсетевого экрана:

1. В меню перейдите в раздел **SD-WAN → Зоны межсетевого экрана**.

   Отобразится таблица общих зон межсетевого экрана.

2. Нажмите на общую зону межсетевого экрана, которую вы хотите удалить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Общая зона межсетевого экрана будет удалена и перестанет отображаться в таблице.

Удаление зоны межсетевого экрана на устройстве CPE

Чтобы удалить зону межсетевого экрана на устройстве CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите удалить зону межсетевого экрана.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Межсетевой экран → Зоны**.

   Отобразится таблица зон межсетевого экрана.

4. Установите флажок **Переопределить**.

5. Нажмите на кнопку **Удалить** рядом с зоной межсетевого экрана, которую вы хотите удалить.

6. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Зона межсетевого экрана будет удалена и перестанет отображаться в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Работа с шаблонами межсетевого экрана

Вы можете посмотреть таблицу шаблонов межсетевого экрана в разделе **SD-WAN → Шаблоны межсетевого экрана**. По умолчанию создан шаблон межсетевого экрана **Default firewall template**, на основании которого создаются остальные шаблоны межсетевого экрана. Информация о шаблонах межсетевого экрана отображается в следующих столбцах таблицы:

- **Имя** – имя шаблона межсетевого экрана.
- **Использование** – использование шаблона межсетевого экрана устройствами CPE:
  - **Да**.
  - **Нет**.
- **Владелец** – имя пользователя, который создал шаблон межсетевого экрана.
- **Последнее обновление** – дата и время последнего изменения параметров шаблона межсетевого экрана.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Вы можете выбрать назначенный шаблон межсетевого экрана, чтобы он был предварительно выбран при добавлении и ручной регистрации устройства CPE.

Параметры шаблона межсетевого экрана можно настроить на следующих вкладках:

- **Основные параметры** – основные параметры межсетевого экрана.
- **Правила** – правила межсетевого экрана.
- **NAT** – параметры трансляции сетевых адресов. На этой вкладке отображаются следующие вкладки:
  - **DNAT** – DNAT-правила.
  - **SNAT** – SNAT-правила.

- **Передачи между зонами** – передачи между зонами межсетевого экрана.
- **Наборы IP** – наборы IP.

Создание шаблона межсетевого экрана

Чтобы создать шаблон межсетевого экрана:

1. Перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**.

   Отобразится таблица шаблонов межсетевых экранов.

2. В верхней части страницы нажмите на кнопку **+ Шаблон межсетевого экрана**.

3. В открывшемся окне введите имя шаблона межсетевого экрана.

4. Нажмите на кнопку **Создать**.

   Шаблон межсетевого экрана будет создан и отобразится в таблице.

Вам нужно настроить созданный шаблон межсетевого экрана. Более подробно о работе с шаблонами межсетевого экрана см. в разделе Работа с шаблонами межсетевого экрана.

Выбор назначенного шаблона межсетевого экрана

Вы можете выбрать назначенный шаблон межсетевого экрана, чтобы он был предварительно выбран при добавлении и ручной регистрации устройства CPE.

Чтобы выбрать назначенный шаблон межсетевого экрана:

1. Перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**.

   Отобразится таблица шаблонов межсетевого экрана.

2. Нажмите на шаблон межсетевого экрана, который вы хотите сделать назначенным шаблоном межсетевого экрана.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры шаблона межсетевого экрана.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Установить назначенным**.

   Шаблон межсетевого экрана станет назначенным шаблоном межсетевого экрана.

Импорт шаблона межсетевого экрана

Вы можете экспортировать шаблон межсетевого экрана, после чего импортировать его в другой шаблон межсетевого экрана. Параметры шаблона межсетевого экрана выстраиваются в соответствии с параметрами импортированного шаблона межсетевого экрана. При импорте можно выбрать вкладки, которые вы хотите оставить без изменений. Шаблон межсетевого экрана, в который был импортирован другой шаблон межсетевого экрана, остается примененным к устройствам CPE, но параметры устройств CPE не изменяются.

Чтобы импортировать шаблон межсетевого экрана:

1. Перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**.

   Отобразится таблица шаблонов межсетевого экрана.

2. Нажмите на шаблон межсетевого экрана, который вы хотите экспортировать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры шаблона межсетевого экрана.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Экспортировать**.

   На ваше локальное устройство сохранится архив в формате TAR.GZ. В архиве не содержится информация об устройствах CPE, использующих шаблон межсетевого экрана.

4. Нажмите на шаблон межсетевого экрана, в который вы хотите импортировать шаблон межсетевого экрана.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⩓. По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры шаблона межсетевого экрана.

5. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Импортировать**.

6. В открывшемся окне снимите флажки рядом с вкладками шаблона межсетевого экрана, которые вы хотите оставить без изменения после импорта.

7. В поле **Файл** укажите путь к архиву в формате TAR.GZ.

8. Нажмите на кнопку **Импортировать**.

Параметры шаблона межсетевого экрана будут изменены в соответствии с параметрами импортированного шаблона межсетевого экрана.

Клонирование шаблона межсетевого экрана

Вы можете клонировать шаблон межсетевого экрана, чтобы создать такой же шаблон межсетевого экрана с другим именем.

Чтобы клонировать шаблон межсетевого экрана:

1. Перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**.

   Отобразится таблица шаблонов межсетевого экрана.

2. Нажмите на шаблон межсетевого экрана, который вы хотите клонировать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры шаблона межсетевого экрана.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Клонировать**.

4. В открывшемся окне введите имя нового шаблона межсетевого экрана.

5. Нажмите на кнопку **Клонировать**.

Клон шаблона межсетевого экрана с новым именем будет создан и отобразится в таблице.

Просмотр использования шаблона межсетевого экрана

При необходимости вы можете посмотреть, какие устройства CPE используют шаблон межсетевого экрана. Например, если шаблон межсетевого экрана используется, его невозможно удалить.

Чтобы посмотреть, используется ли шаблон межсетевого экрана:

1. Перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**.

   Отобразится таблица шаблонов межсетевого экрана.

2. Нажмите на шаблон межсетевого экрана, использование которого вы хотите посмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры шаблона межсетевого экрана.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Показать связанные CPE**.

Откроется окно с таблицей устройств CPE, использующих шаблон межсетевого экрана.

Удаление шаблона межсетевого экрана

Вы не можете удалить шаблон межсетевого экрана, если он используется хотя бы одним устройством CPE. Для удаления шаблона межсетевого экрана, который используется устройствами CPE, вам нужно сначала изменить шаблон межсетевого экрана устройств CPE. Вы можете посмотреть, какие устройства CPE используют шаблон межсетевого экрана.

Удаленные шаблоны межсетевого экрана невозможно восстановить.

Чтобы удалить шаблон межсетевого экрана:

1. Перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**.

   Отобразится таблица шаблонов межсетевого экрана.

2. Нажмите на шаблон межсетевого экрана, который вы хотите удалить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры шаблона межсетевого экрана.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Шаблон межсетевого экрана будет удален и перестанет отображаться в таблице.

Настройка основных параметров межсетевого экрана

Вы можете настроить основные параметры межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Основные параметры межсетевого экрана, указанные в шаблоне межсетевого экрана, автоматически распространяются на все устройства CPE, которые используют шаблон межсетевого экрана.

Межсетевой экран применяет к пакетам трафика действия, указанные в основных параметрах межсетевого экрана. Это происходит, если к пакетам трафика не было применено ни одно из правил межсетевого экрана, и пакеты не были переданы ни в одну из зон межсетевого экрана.

Чтобы настроить основные параметры межсетевого экрана:

1. Перейдите к настройке основных параметров межсетевого экрана одним из следующих способов:

   - Если вы хотите настроить основные параметры межсетевого экрана в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана** и нажмите на шаблон межсетевого экрана.

   - Если вы хотите настроить основные параметры межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран** и установите флажок **Переопределить**.

   По умолчанию выбрана вкладка **Основные параметры**, на которой отображаются основные параметры межсетевого экрана.

2. Если вы хотите выключить защиту от SYN-флуда, снимите флажок **Защита от Syn-flood**. Этот флажок установлен по умолчанию. Когда защита от SYN-флуда включена, на устройство CPE раз в секунду может передаваться не более 25 пакетов трафика с флагами SYN, ACK, RST и FIN.

3. Если вы хотите, чтобы межсетевой экран отбрасывал входящие на устройство CPE пакеты трафика, отмеченные функцией conntrack как неправильные, установите флажок **DROP неправильных пакетов**. Этот флажок снят по умолчанию.

4. Если вы хотите выключить использование технологии DPI (Deep Packet Inspection), снимите флажок **Включить DPI**. Этот флажок установлен по умолчанию. С помощью технологии DPI вы можете создавать правила межсетевого экрана, которые применяются только к пакетам трафика указанного приложения.

   Когда использование технологии DPI выключено, вы не можете настроить маркировку DPI, и правила межсетевого экрана, которые используют технологию DPI, автоматически выключаются.

5. В раскрывающемся списке **INPUT-действие по умолчанию** выберите действие, которое межсетевой экран выполняет со входящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Это значение выбрано по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

6. В раскрывающемся списке **OUTPUT-действие по умолчанию** выберите действие, которое межсетевой экран выполняет с исходящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Это значение выбрано по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

7. В раскрывающемся списке **FORWAD-действие по умолчанию** выберите действие, которое межсетевой экран выполняет с пакетами трафика, пересылаемыми между сетевыми интерфейсами и подсетями:

   - **ACCEPT** – принимать пакеты трафика. Это значение выбрано по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

8. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Настройка маркировки DPI

Kaspersky SD-WAN поддерживает создание правил межсетевого экрана, которые применяются только к пакетам трафика указанного приложения. Вы можете указать марки DPI, на основании которых правила межсетевого экрана применяются к пакетам трафика. Вы не можете настроить маркировку DPI, если вы выключили использование технологии DPI при настройке основных параметров межсетевого экрана.

Вы можете настроить маркировку DPI в шаблоне межсетевого экрана или на устройстве CPE. Параметры маркировки DPI, указанные в шаблоне межсетевого экрана, автоматически распространяются на все устройства CPE, которые используют шаблон межсетевого экрана.

Чтобы настроить маркировку DPI:

1. Перейдите к настройке маркировки DPI для межсетевого экрана одним из следующих способов:

   - Если вы хотите настроить маркировку DPI в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Маркировка DPI**.

   - Если вы хотите настроить маркировку DPI на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Маркировка DPI** и установите флажок **Переопределить**.

   Отобразятся параметры маркировки DPI.

2. Установите флажки рядом с марками DPI, на основании которых правила межсетевого экрана применяются к пакетам трафика.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с правилами межсетевого экрана

Вы можете посмотреть таблицу правил межсетевого экрана в шаблоне межсетевого экрана и на устройстве CPE:

- Для просмотра таблицы правил межсетевого экрана в шаблоне межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажать на шаблон межсетевого экрана и выбрать вкладку **Правила**.

- Для просмотра таблицы правил межсетевого экрана на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Межсетевой экран → Правила**.

По умолчанию созданы следующие правила межсетевого экрана:

- **Allow-GENEVE** – разрешает устройству CPE получать GENEVE-пакеты из WAN-зоны межсетевого экрана. GENEVE-пакеты являются инкапсулированным трафиком Kaspersky SD-WAN.

- **Allow-DHCP-Renew** – разрешает устройству CPE получать BOOTP-пакеты из WAN-зоны межсетевого экрана для правильной работы протокола DHCP.

- **Allow-IGMP** – разрешает устройству CPE получать IGMP-пакеты из WAN-зоны межсетевого экрана для правильной работы протоколов VRRP и multicast.

- Следующие правила межсетевого экрана временно выключены до появления полной поддержки протокола IPv6 в Kaspersky SD-WAN:
  - **Allow-DHCPv6** – разрешает устройству CPE получать DHCPv6-пакеты из WAN-зоны межсетевого экрана для правильной работы протокола IPv6.
  - **Allow-MLD** – разрешает устройству CPE получать MLD-пакеты из WAN-зоны межсетевого экрана для правильной работы протокола IPv6.
  - **Allow-ICMPv6-Input** – разрешает устройству CPE получать ICMPv6-пакеты из WAN-зоны межсетевого экрана для правильной работы протокола IPv6.
  - **Allow-ICMPv6-Forward-From-Wan** – разрешает устройству CPE получать ICMPv6-пакеты из WAN-зоны межсетевого экрана, которые пересылаются в LAN-зону межсетевого экрана, для правильной работы протокола IPv6.
  - **Allow-ICMPv6-Forward-From-Lan** – разрешает устройству CPE получать ICMPv6-пакеты из LAN-зоны межсетевого экрана, которые пересылаются в WAN-зону межсетевого экрана, для правильной работы протокола IPv6.
- **Explicit-deny-http-on-wan** – запрещает устройству CPE получать пакеты трафика протокола TCP с портом назначения 80 для предотвращения доступа из WAN-зоны межсетевого экрана к веб-серверу устройства CPE.
- **Explicit-deny-https-on-wan** – запрещает устройству CPE получать пакеты трафика протокола TCP с портом назначения 443 для предотвращения доступа из WAN-зоны межсетевого экрана к веб-серверу устройства CPE.

Для правильной работы правил межсетевого экрана по умолчанию вам нужно добавить сетевые интерфейсы **sd-wan<0–4>** в WAN-зону межсетевого экрана. Вы можете добавить сетевые интерфейсы в зону межсетевого экрана при создании или изменении сетевых интерфейсов.

Информация о правилах межсетевого экрана отображается в следующих столбцах таблицы:

- **Имя** – имя правила межсетевого экрана.
- **Детали** – критерии, согласно которым межсетевой экран применяет правило к пакетам трафика.
- **Действие** – действие, которое правило межсетевого экрана выполняет с пакетами трафика.

Создание правила межсетевого экрана

Вы можете создать правило межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Правило межсетевого экрана, созданное в шаблоне межсетевого экрана, автоматически создается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы создать правило межсетевого экрана:

1. Перейдите к созданию правила межсетевого экрана одним из следующих способов:

   - Если вы хотите создать правило межсетевого экрана в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Правила**.

   - Если вы хотите создать правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Правила** и установите флажок **Переопределить**.

   Отобразится таблица правил межсетевого экрана.

2. Нажмите на кнопку **+ Правило**.

3. В открывшемся окне в поле **Имя** введите имя правила межсетевого экрана. Максимальная длина имени: 255 символов.

4. В раскрывающемся списке **Действие** выберите действие, которое правило межсетевого экрана выполняет с пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Это значение выбрано по умолчанию.

   - **DROP** – отбрасывать пакеты трафика.

   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

   - **ADJ-MSS** – изменять значение в поле MSS в TCP-заголовке пакетов трафика на указанное значение MSS. При выборе этого значения в поле **Величина MSS** введите значение MSS. Диапазон значений: от 68 до 10 000.

5. Укажите критерии, согласно которым межсетевой экран применяет правило межсетевого экрана к пакетам трафика:

   a. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанными IP-адресами или подсетями источника или назначения, в раскрывающемся списке **Набор IP** выберите созданный набор IP. При выборе значения в этом раскрывающемся списке становятся недоступны блоки **IP источника** и **IP назначения**.

   b. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с версией IP-адресов или подсетей источника или назначения IPv4, в раскрывающемся списке **Версия IP** выберите **IPv4**. Если не выбрать значение, правило межсетевого экрана применяется к пакетам трафика с любой версией IP-адресов или подсетей источника или назначения.

   c. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанной зоной межсетевого экрана источника, в раскрывающемся списке **Зона источника** выберите созданную зону межсетевого экрана.

   d. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанной зоной межсетевого экрана назначения, в раскрывающемся списке **Зона назначения** выберите созданную зону межсетевого экрана.

   e. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанным IPv4-адресом или префиксом источника, в блоке **IP источника** нажмите на кнопку **+ Добавить** и введите IPv4-адрес или префикс источника.

      IPv4-адрес или префикс будет указан и отобразится в блоке **IP источника**. Вы можете указать несколько IPv4-адресов или префиксов и удалить IPv4-адреса или префиксы. Для удаления IPv4-адреса или префикса нажмите рядом с ним на значок удаления ✕.

   f. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанным IPv4-адресом или префиксом назначения, в блоке **IP назначения** нажмите на кнопку **+ Добавить** и введите IPv4-адрес или префикс назначения.

      IPv4-адрес или префикс будет указан и отобразится в блоке **IP назначения**. Вы можете указать несколько IPv4-адресов или префиксов и удалить IPv4-адреса или префиксы. Для удаления IPv4-адреса или префикса нажмите рядом с ним на значок удаления ✕.

   g. Если вы хотите применять правило межсетевого экрана только к пакетам трафика указанного протокола, в раскрывающемся списке **Протокол** выберите протокол. При выборе значения в этом раскрывающемся списке становится недоступным раскрывающийся список **DPI протокол**.

      Если вы выбрали **TCP** или **UDP** и хотите применять правило межсетевого экрана только к пакетам трафика с указанными портами источника и/или назначения, выполните следующие действия:

      1. В поле **Порт источника** введите номер порта источника или диапазон номеров порта источника.
      2. В поле **Порт назначения** введите номер порта назначения или диапазон номеров порта назначения.

      Диапазон значений: от 0 до 65 535. Формат диапазона номеров портов: `<первое значение>-<последнее значение>`. Например, вы можете ввести `10` или `10-15`.

   h. Если вы хотите применять правило межсетевого экрана только к пакетам трафика указанного приложения, в раскрывающемся списке **DPI протокол** выберите приложение.

      Трафик приложения определяется с помощью технологии DPI, которая создает дополнительную нагрузку на процессор устройства CPE.

Вы можете указать марки DPI, на основании которых правило межсетевого экрана применяется к пакетам трафика. Если вы выключили использование технологии DPI при настройке основных параметров межсетевого экрана, правило межсетевого экрана автоматически выключается.

6. Нажмите на кнопку **Создать**.

   Правило межсетевого экрана будет создано и отобразится в таблице.

7. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

По умолчанию правило межсетевого экрана выключено. Вам нужно включить правило межсетевого экрана, чтобы оно применялось к пакетам трафика.

Настройка порядка применения правил межсетевого экрана

Правила межсетевого экрана применяются к пакетам трафика по порядку, начиная с первого правила межсетевого экрана в верхней части таблицы. По умолчанию правила межсетевого экрана отображаются в таблице в порядке создания. Чем раньше правило межсетевого экрана было создано, тем выше оно отображается в таблице.

Вы можете настроить порядок применения правил межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Порядок применения правил межсетевого экрана, указанный в шаблоне межсетевого экрана, автоматически распространяется на все устройства CPE, которые используют шаблон межсетевого экрана.

Чтобы настроить порядок применения правил межсетевого экрана:

1. Перейдите к настройке порядка применения правил межсетевого экрана одним из следующих способов:

   - Если вы хотите настроить порядок применения правил межсетевого экрана в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Правила**.

   - Если вы хотите настроить порядок применения правил межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Правила** и установите флажок **Переопределить**.

   Отобразится таблица правил межсетевого экрана.

2. Настройте порядок применения правил межсетевого экрана, нажимая рядом с ними на кнопки **Вверх** и **Вниз**.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Включение и выключение правила межсетевого экрана

По умолчанию созданные правила межсетевого экрана выключены. Вам нужно включить правило межсетевого экрана, чтобы оно применялось к пакетам трафика.

Вы можете включить или выключить правило межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Правило межсетевого экрана, включенное или выключенное в шаблоне межсетевого экрана, автоматически включается или выключается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы включить или выключить правило межсетевого экрана:

1. Перейдите к включению или выключению правила межсетевого экрана одним из следующих способов:

   - Если вы хотите включить или выключить правило межсетевого экрана в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Правила**.

   - Если вы хотите включить или выключить правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Правила** и установите флажок **Переопределить**.

   Отобразится таблица правил межсетевого экрана.

2. Нажмите на кнопку **Включить** или **Выключить** рядом с правилом межсетевого экрана, которое вы хотите включить или выключить.

   Правило межсетевого экрана будет включено или выключено.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Изменение правила межсетевого экрана

Вы можете изменить правило межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Правило межсетевого экрана, измененное в шаблоне межсетевого экрана, автоматически изменяется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы изменить правило межсетевого экрана:

1. Перейдите к изменению правила межсетевого экрана одним из следующих способов:

   - Если вы хотите изменить правило межсетевого экрана в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Правила**.

   - Если вы хотите изменить правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Правила** и установите флажок **Переопределить**.

   Отобразится таблица правил межсетевого экрана.

2. Нажмите на кнопку **Изменить** рядом с правилом межсетевого экрана, которое вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры правила межсетевого экрана. Описание параметров см. в инструкции по созданию правила межсетевого экрана.

4. Нажмите на кнопку **Сохранить**.

   Правило межсетевого экрана будет изменено и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Удаление правила межсетевого экрана

Вы можете удалить правило межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Правило межсетевого экрана, удаленное в шаблоне межсетевого экрана, автоматически удаляется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Удаленные правила межсетевого экрана невозможно восстановить.

Чтобы удалить правило межсетевого экрана:

1. Перейдите к удалению правила межсетевого экрана одним из следующих способов:

   - Если вы хотите удалить правило межсетевого экрана в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN** → **Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Правила**.

   - Если вы хотите удалить правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран** → **Правила** и установите флажок **Переопределить**.

   Отобразится таблица правил межсетевого экрана.

2. Нажмите на кнопку **Удалить** рядом с правилом межсетевого экрана, которое вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Правило межсетевого экрана будет удалено и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с расширенными правилами межсетевого экрана

Расширенные правила реализуют модель классического пакетного фильтра типа iptables. На рисунке ниже показана схема обработки пакетов расширенными правилами:

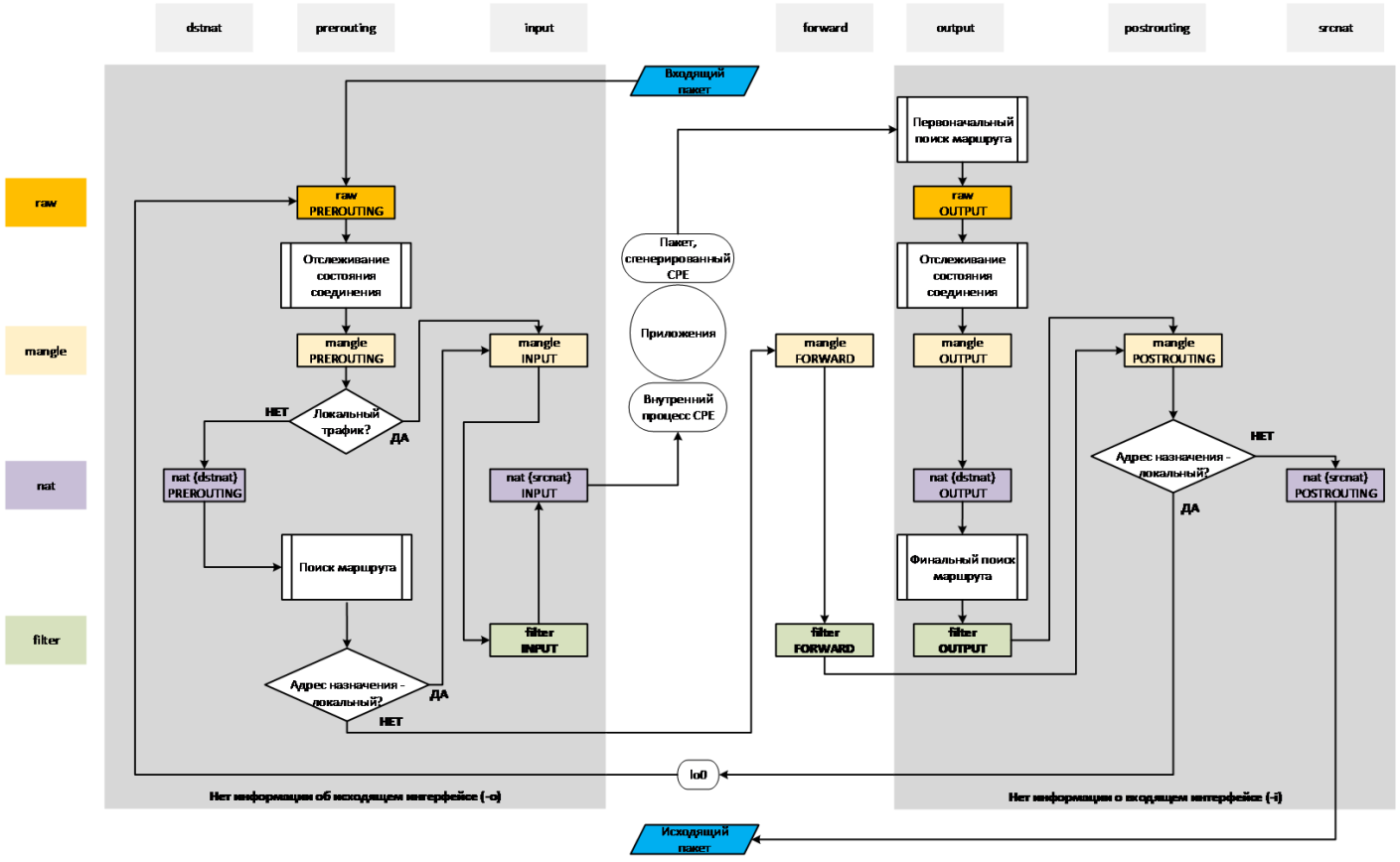


Схема обработки пакетов расширенными правилами по модели классического пакетного фильтра типа iptables

Вы можете просматривать таблицу расширенных правил межсетевого экрана в шаблоне межсетевого экрана и на устройстве CPE:

- Для просмотра таблицы расширенных правил межсетевого экрана в шаблоне межсетевого экрана в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Расширенные правила**.

- Для просмотра таблицы расширенных правил межсетевого экрана на устройстве CPE в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE и выберите вкладку **Межсетевой экран → Расширенные правила**.

Дополнительные критерии совпадения для расширенных правил

В расширенных правилах межсетевого экрана можно использовать дополнительные критерии совпадения для отбора пакетов. Этот раздел содержит описание этих критериев и их параметров.

Фрагментированный пакет

Критерий срабатывает при обнаружении в трафике фрагментов IP-пакетов, за исключением первого фрагмента. Такие пакеты предварительно помечаются специальной меткой, поэтому этот критерий не может использоваться одновременно с критерием **Совпадение по метке**. Включение параметра **Фрагментированный пакет** автоматически отключает параметр **Совпадение по метке**, если он был включен, и блокирует его.

Совпадение по метке

Критерий срабатывает при обнаружении в пакетах поля с меткой, установленной ранее с помощью действия `MARK`.

Параметры:

Значение

Значение метки в шестнадцатеричном (`0x0-0xFFFFFFFF`) или десятичном (`0-4294967295`) формате.

Примеры: `0x1`; `1`

Маска

Необязательное значение битовой маски в шестнадцатеричном (`0x0-0xFFFFFFFF`) или десятичном (`0-4294967295`) формате. Если указано, применяется к метке с помощью логического И для указания битов, которые должны совпадать.

Пример: `0xFF`

TOS

Критерий срабатывает при обнаружении в пакетах заданного значения поля `TOS (Type of Service)` в IPv4-заголовке пакета.

Параметры:

Значение

Значение TOS в шестнадцатеричном (`0x0-0xFF`) или десятичном (`0-255`) формате.

Маска

Необязательное значение битовой маски в шестнадцатеричном (`0x0-0xFF`) или десятичном (`0-255`) формате. Если указано, применяется к значению поля `TOS` с помощью логического И для указания битов, которые должны совпадать.

Совпадение по строке

Критерий срабатывает при обнаружении в пакете указанных символов в текстовой или шестнадцатеричной записи.

Параметры:

Паттерн для поиска

Поисковый шаблон в текстовом или шестнадцатеричном представлении. Максимальная длина – 255 символов. Поддерживаются следующие символы:

- Верхний регистр (A-Z)
- Нижний регистр (a-z)
- Цифры (0-9)
- Специальные символы (_ - . , : ; / + = @ ( ) ! ?)
- Пробел

Алгоритм

Алгоритм сравнения строк для поиска:

- BM (алгоритм Бойера – Мура)
- KMP (алгоритм Кнута – Морриса – Пратта).

Диапазон позиций

Диапазон байтов в пакете, в котором выполняется поиск совпадений строк. Позиции байтов отсчитываются от 0. Если не указано, используется размер пакета.

HEX-строка

Если включено, значение в поле **Паттерн для поиска** используется как строка в шестнадцатеричном представлении.

Игнорировать регистр

Если включено, регистр символов игнорируется.

Совпадение по недавним

Критерий применяется на основе предыдущей активности соединений. Если параметр включен, позволяет динамически создавать список IP-адресов, затем сверять пакеты по этому списку.

Параметры:

Имя списка

Имя списка для сопоставления.

Действие

Требуемое действие со списком:

- `set` (добавить IP-адрес в список)
- `rcheck` (проверить наличие IP-адреса в списке без обновления времени)
- `update` (проверить наличие IP-адреса и обновить время)
- `update` (проверить наличие IP-адреса в списке и обновить время)
- `remove` (удалить IP-адрес из списка)

Недопустимые TCP-флаги

Критерий срабатывает при обнаружении в пакетах недопустимых комбинаций TCP-флагов, обычно используемых в техниках сканирования подсетей.

При включении этого параметра значение поля **Протокол** в разделе **Общие** автоматически устанавливается в `TCP`.

Параметры:

Комбинации флагов

Позволяет выбрать нужные комбинации флагов в зависимости от распространенных техник сканирования:

- Все флаги (сканирование TCP ALL)
- Пустые флаги (сканирование TCP NULL)
- Флаги FIN+ACK (сканирование Мэймона)
- Флаг ACK в неустановленной сессии (сканирование TCP ACK)
- Флаги FIN+PSH+URG (Xmas-сканирование)

Ограничение частоты

Критерий срабатывает, если скорость поступления пакетов в секунду не превышает заданное ограничение на основе алгоритма "Ведро с токенами".

Параметры:

Ограничение, пакетов/сек.

Задает максимально допустимую частоту пакетов в секунду. Правило с указанным ограничением срабатывает только на трафике, скорость которого не превышает указанное ограничение с учетом всплеска (см. ниже). Пакеты, скорость которых превысила ограничение, не обрабатываются этим правилом.

Всплеск, пакетов

Максимальное количество пакетов, которые могут однократно пройти сверх установленного ограничения. При исчерпании пополняется с постоянной сторостью, равной значению в поле **Ограничение, пакетов/сек.**

Срабатывать на TCP SYN

Дополнительный критерий соответствия для TCP-пакетов, содержащих флаг `SYN`. При включении этого параметра значение поля **Протокол** в разделе **Общие** автоматически устанавливается в `TCP`.

Мобильный код

Критерий срабатывает при обнаружении мобильного кода в незашифрованном HTTP-трафике. Требует включенного DPI для определения HTTP-трафика в том числе на нестандартных портах.

При включении этого параметра автоматически выключаются все другие параметры расширенного сопоставления (параметры **Протокол** и **DPI** в разделе **Главное** и все другие расширенные критерии в разделе **Дополнительные совпадения**.

Параметры:

Типы мобильного кода

Позволяет выбрать один или несколько типов мобильного кода, при обнаружении которых должен срабатывать критерий:

- Java-апплеты
- Сборки WebAsm
- Скрипты JavaScript/ECMA
- Скрипты JavaScript в теле страницы
- Элементы ActiveX
- Скрипты/документы PDF
- Скрипты/документы PostScript
- Анимации/скрипты Adobe Flash
- Скрипты VB/VBA

Совпадение по командам протоколов прикладного уровня

Критерий срабатывает при обнаружении в незашифрованном трафике указанных команд определенных протоколов прикладного уровня. Для использования этого критерия необходимо включить функцию DPI в основных параметрах межсетевого экрана.

Вы можете указать следующие протоколы прикладного уровня и их команды:

Протокол	Команда
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 LIST RETR DELE NOOP RSET TOP UIDL
FTP control	USER PASS QUIT LIST RETR STOR DELE RMD REMOVE DIRECTORY MKD MAKE DIRECTORY PASV EPSV

Вы можете использовать этот критерий при создании или изменении расширенных правил межсетевого экрана. Для этого в разделе **Общие** области настройки параметров расширенного правила включите переключатель **DPI**, выберите нужный протокол прикладного уровня в выпадающем списке **Конкретный протокол**, затем выберите нужную команду в выпадающем списке **Команда**. При выборе значения Любой критерий будет срабатывать при наличии любой из перечисленных команд в выбранном протоколе.

Создание расширенного правила

Вы можете создавать расширенные правила в шаблонах межсетевого экрана или на устройствах CPE. Расширенные правила, созданные в шаблоне межсетевого экрана, автоматически создаются на всех устройствах CPE, которые используют этот шаблон.

Чтобы создать расширенное правило:

1. Перейдите к созданию расширенного правила одним из следующих способов:

   - Чтобы создать расширенное правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Расширенные правила**.

   - Если вы хотите создать правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Расширенные правила** и включите переключатель **Переопределить**.

   Отобразится таблица расширенных правил межсетевого экрана.

2. Нажмите на кнопку **+ Добавить**.

   Откроется окно создания расширенного правила.

3. Настройте основные параметры в разделе **Общие**.

   a. Введите имя расширенного правила в поле **Имя**. Максимальная длина имени – 255 символов. Допустимые символы: A-Z, a-z, 0-9, _ - . , : ; / + = @ ( ) ! ? и пробел.

   b. При необходимости введите описание расширенного правила в поле **Описание**.

   c. При необходимости укажите один или несколько тегов политик, выбрав их в раскрывающемся списке **Теги политик**. Помеченное тегом правило по умолчанию становится неактивным. Вы можете активировать его позже.

      С помощью тегов политик вы можете одновременно включать или выключать набор правил, решающих определенную задачу. Также вы можете интегрировать внешнюю систему защиты информации и включать или выключать теги политик через API.

   d. Укажите таблицу межсетевого экрана, в которую вы хотите добавить расширенное правило, выбрав ее в выпадающем списке **Таблица**. Доступны следующие таблицы:

      - FILTER
      - MANGLE
      - NAT
      - RAW

   e. Для выбранной таблицы укажите цепочку, в которую вы хотите добавить расширенное правило, выбрав ее в выпадающем списке **Цепочка**. Набор доступных цепочек зависит от выбранной на предыдущем шаге таблицы:

      - FILTER
        - INPUT
        - FORWARD
        - OUTPUT
      - MANGLE
        - INPUT
        - FORWARD
        - OUTPUT
        - PREROUTING
        - POSTROUTING
      - NAT
        - PREROUTING
        - POSTROUTING

- INPUT
- OUTPUT

- RAW
  - OUTPUT
  - PREROUTING

f. При необходимости укажите протокол, для которого должно применяться расширенное правило, выбрав нужное значение в выпадающем списке **Протокол**:

- TCP
- UDP
- ICMP
- Все (правило применяется ко всем перечисленным выше протоколам)

Если в качестве протокола вы выбрали ICMP, укажите тип и код ICMP-пакета, на которых должно срабатывать правило. Для этого в полях **Тип** и **Код** введите значение от `0` до `255`.

g. При необходимости настройте сопоставление по DPI:

1. Включите переключатель **DPI**.
2. Укажите прикладной протокол или идентификатор сервиса/приложения, на котором должно срабатывать правило, выбрав нужное значение из списка **Конкретный протокол**.
3. При необходимости настройте сопоставление по командам протоколов прикладного уровня, если в качестве критерия сопоставления по DPI вы выбрали один из следующих протоколов: `HTTP`, `SMTP`, `SIP`, `IMAP`, `POP3`, `FTP control`.

> Вы не можете использовать сопоставление по **DPI** одновременно с сопоставлением по параметру **Протокол** из предыдущего шага. При использовании сопоставления по **DPI** параметр **Протокол** блокируется, а указанные для него значения игнорируются.

h. Настройте порядок добавления расширенного правила в список расширенных правил с помощью блока параметров **Размещение правила**:

1. Укажите тип размещения расширенного правила:
   - Предправила (англ. pre-rules) вставляются перед другими;
   - Постправила (англ. post-rules) добавляются после других правил или в конец таблицы.
2. Укажите расположение расширенного правила в таблице:
   - Начало таблицы
   - Конец таблицы

- После указанного расширенного правила

i. При необходимости в соответствующих полях укажите IP-адрес источника и IP-адрес назначения, на которых должно срабатывать правило.

Если необходимо, чтобы правило срабатывало на всех IP-адресах источника или назначения, кроме указанных, установите для соответствующего поля флажок **Сделать исключением**.

j. При необходимости укажите интерфейсы источника или назначения, используя поля в блоке параметров **Интерфейсы**.

k. Укажите целевое действие, которое расширенно правило должно выполнять с пакетом при срабатывании, выбрав нужное значение в выпадающем списке **Цель**:

- ACCEPT
- DROP
- TTL
- REJECT
- MARK
- TOS
- LOG
- RETURN
- DNAT
- CLASSIFY

Состав действий зависит от выбранной таблицы. При выборе действий TTL, MARK, TOS, DNAT, CLASSIFY потребуется также указать дополнительные значения, которые необходимо добавить к пакету.

4. Настройте дополнительные критерии совпадения для расширенного правила в разделе **Дополнительные совпадения**. Подробное описание параметров настройки критериев см. в разделе справки Дополнительные критерии совпадения для расширенных правил.

5. При необходимости просмотрите итоговую команду iptables, которая будет выполнена на устройстве CPE после применения правила, нажав **Просмотр команды** вверху области настройки.

6. Нажмите на кнопку **Создать**.

Расширенное правило будет создано и отобразится в таблице.

7. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Включение и выключение расширенных правил

Вы можете включать или выключать расширенные правила межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Расширенные правила, включенные или выключенные в шаблоне межсетевого экрана, автоматически включаются или выключаются на всех устройствах CPE, которые используют этот шаблон межсетевого экрана.

Чтобы включить или выключить расширенное правило:

1. Перейдите к включению или выключению расширенного правила одним из следующих способов:

   - Чтобы включить или выключить расширенное правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Расширенные правила**.

   - Чтобы включить или выключить расширенное правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Расширенные правила** и включите переключатель **Переопределить**.

   Отобразится таблица расширенных правил.

2. С помощью переключателей переключатель **Выключено** или **Включено** включите или выключите нужные расширенные правила.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Изменение расширенного правила

Вы можете изменять расширенные правила в шаблоне межсетевого экрана или на устройстве CPE. Расширенные правила, измененные в шаблоне межсетевого экрана, автоматически изменяются на всех устройствах CPE, которые используют этот шаблон межсетевого экрана.

Чтобы изменить расширенное правило:

1. Перейдите к изменению расширенного правила одним из следующих способов:

   - Чтобы изменить расширенное правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Расширенные правила**.

   - Чтобы изменить расширенное правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Расширенные правила** и включите переключатель **Переопределить**.

   Отобразится таблица расширенных правил.

2. Выберите в таблице расширенное правило, которое вы хотите изменить, и нажмите на кнопку **Изменить**.

3. В открывшемся окне измените нужные параметры расширенного правила. Описание параметров см. в инструкции по созданию расширенного правила.

4. Нажмите на кнопку **Сохранить**.

   Расширенное правило будет изменено и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Удаление расширенного правила

Вы можете удалять расширенные правила в шаблоне межсетевого экрана или на устройстве CPE. Расширенные правила, удаленные в шаблоне межсетевого экрана, автоматически удаляются на всех устройствах CPE, которые используют этот шаблон межсетевого экрана.

Удаленные расширенные правила невозможно восстановить.

Чтобы удалить расширенные правила:

1. Перейдите к удалению расширенных правил одним из следующих способов:

   - Чтобы удалить расширенные правила в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Расширенные правила**.

   - Чтобы удалить расширенные правила на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Расширенные правила** и включите переключатель **Переопределить**.

   Отобразится таблица расширенных правил.

2. Выберите в таблице одно или несколько расширенных правил, которые вы хотите удалить, и нажмите.на кнопку **Удалить**.

3. Подтвердите удаление, нажав в открывшемся окне на кнопку **Удалить**.

   Расширенные правила будут удалены и перестанут отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

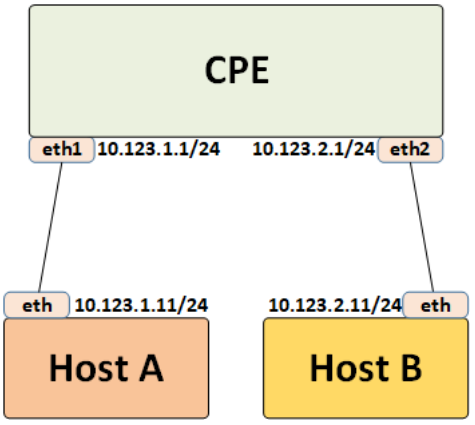
Клонирование расширенного правила

Сценарий: скрытие устройства CPE на пути прохождения трафика с помощью расширенных правил межсетевого экрана

При размещении устройства CPE на удаленной площадке у администраторов часто отсутствует полный контроль над действиями пользователей внутренней сети, где расположено устройство CPE. В такой ситуации вам может потребоваться исключить возможность обнаружения устройства CPE как активного узла сети при сканировании из внутренней сети. Вы можете скрыть устройство CPE в топологии сети с помощью расширенных правил межсетевого экрана.

В этом сценарии описаны шаги для создания расширенных правил, позволяющих скрыть устройство CPE от обнаружения стандартными средствами сканирования сети.

Исходное состояние



Топология сети

Исходное состояние компонентов сети выглядит следующим образом:

- Два хоста A и B подключены к устройству CPE.
- Интерфейсы `eth1` и `eth2` на устройстве CPE находятся в одной зоне.
- Межсетевые экраны на хостах A и B настроены на пропуск трафика ICMP.

- С хоста A выполняется трассировка маршрута до хоста B с помощью `traceroute`:

```
tracert -d 10.123.2.11
```

Результат:

```
1 10.123.1.1
2 10.123.2.11
```

Интерпретация результата:

Трассировка маршрутов показывает промежуточный узел между хостами, которым является устройство CPE.

- Анализ сетевого трафика на CPE для протокола ICMP между хостами A и B с помощью команды `tcpdump -i any net 10.123.0.0/16` показывает следующее:

```
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
```

Интерпретация:

Что делает traceroute	Как это выглядит в tcpdump	Что происходит на CPE
Отправляет ICMP Echo Request (или UDP-пакет) с TTL = 1 к целевому IP 10.123.2.11 (хост B).	In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 102...	Маршрутизатор получает пакет, уменьшает TTL до 0, отбрасывает его и генерирует ICMP Time-Exceeded обратно к источнику.
Получает от маршрутизатора ICMP Time-Exceeded (source = router 10.123.1.1).	Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit...	Это первый хоп в выводе traceroute – адрес маршрутизатора.
Увеличивает TTL до 2 и посылает новый запрос.	In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, seq 103...	TTL = 2 позволяет пакету пройти через маршрутизатор (TTL-1=1), но маршрутизатор все еще не знает MAC-адреса конечного хоста, поэтому делает ARP-запрос к 10.123.2.11.
ARP Request от маршрутизатора (10.123.2.1) → 10.123.2.11.	Out ARP, Request who-has 10.123.2.11 tell 10.123.2.1	маршрутизатор пытается разрешить MAC-адрес хоста B в своей второй подсети.
ARP Reply от 10.123.2.11.	In ARP, Reply 10.123.2.11 is-at bc:24:11:59:58:b7	После получения MAC-адреса хоста B маршрутизатор отправляет пакет дальше.

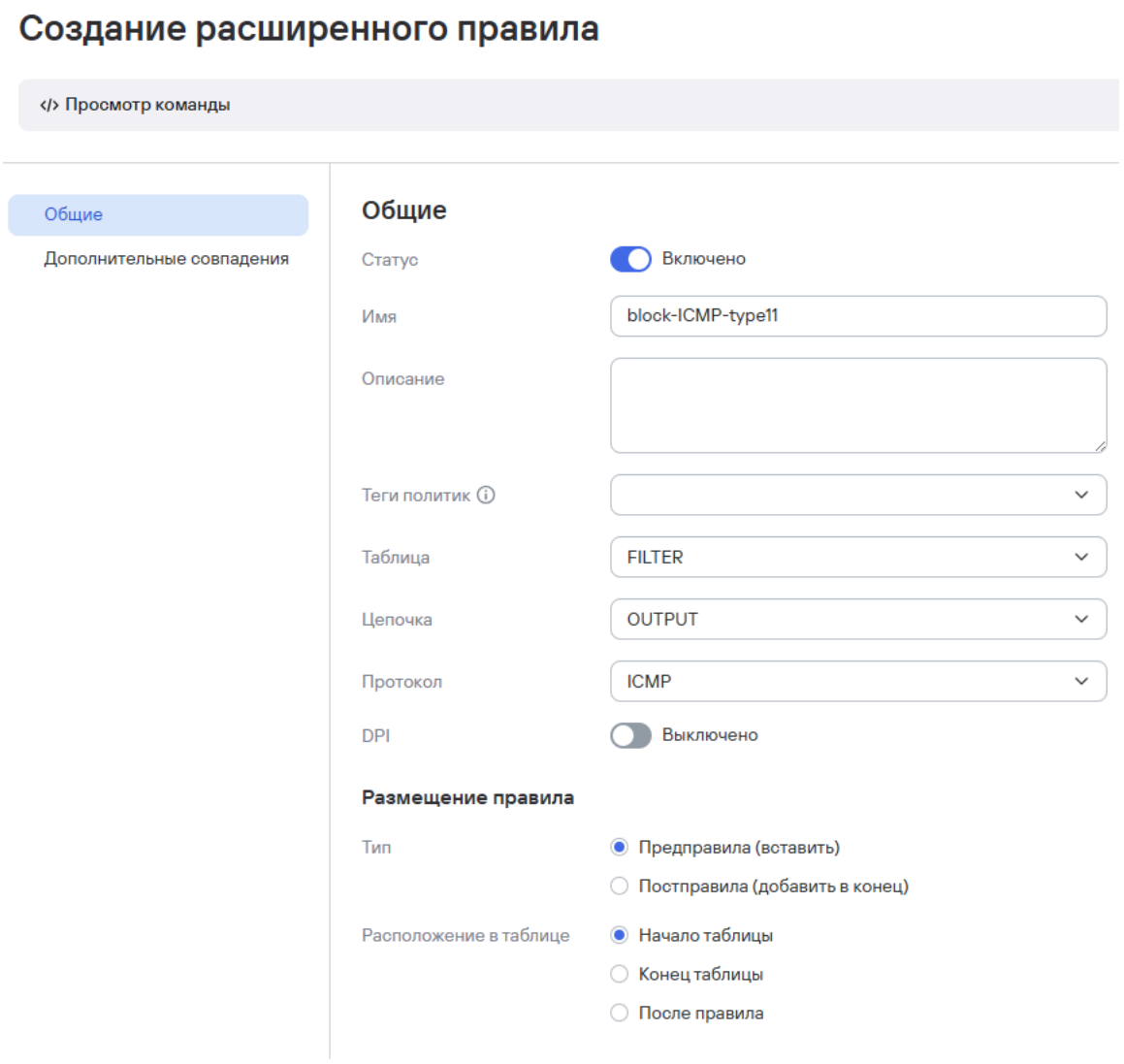
Пакет с TTL = 2 уже дошел до конечного хоста (TTL-1 = 1), поэтому маршрутизаторне генерирует Time-Exceeded, а просто форвардит его.	Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, seq 105…	Хост B получает запрос и отвечает ICMP echo reply.
ICMP Echo Reply от 10.123.2.11 → 10.123.1.11.	In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply…	traceroute получает ответ и выводит второй хоп – адрес хоста B.

Таким образом, сценарий скрытия устройства CPE от обнаружения в сети состоит из следующих шагов:

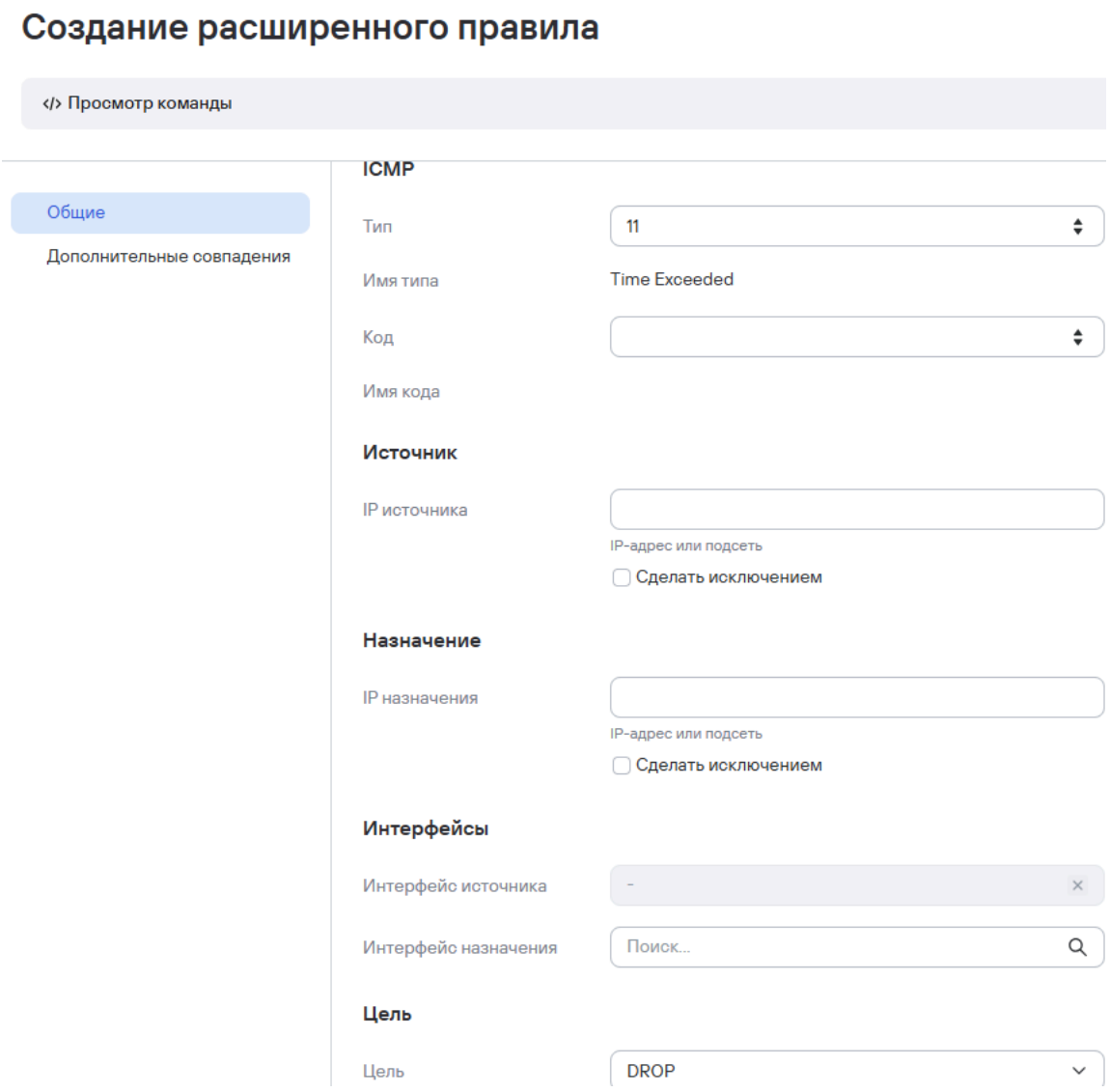
1. **Скрытие CPE из вывода traceroute**

a. Создайте на устройстве CPE расширенное правило, которое блокирует генерируемые на CPE

исходящие сообщения `ICMP Time-Exceeded`, когда CPE получает IP-пакет с `TTL=1`:



Создание расширенного правила для блокировки сообщений ICMP Time-Exceeded 1



Создание расширенного правила для блокировки сообщений ICMP Time-Exceeded 2

Созданное расширенное правило соответствует следующей команде в формате iptables:

```
iptables -t filter -I OUTPUT -p icmp --icmp-type 11 -j DROP -m comment --comment "#ADV Name: block-ICMP-type11"
```

Аналогичное правило в формате iptables при выводе `iptables -L` выглядит следующим образом:

```
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. Проверьте трассировку маршрута от хоста A до хоста B:

На хосте A выполните трассировку маршрута до хоста B:

```
tracert -d 10.123.2.11
```

Результат:

```
1 Request timed out
2 10.123.2.11
```

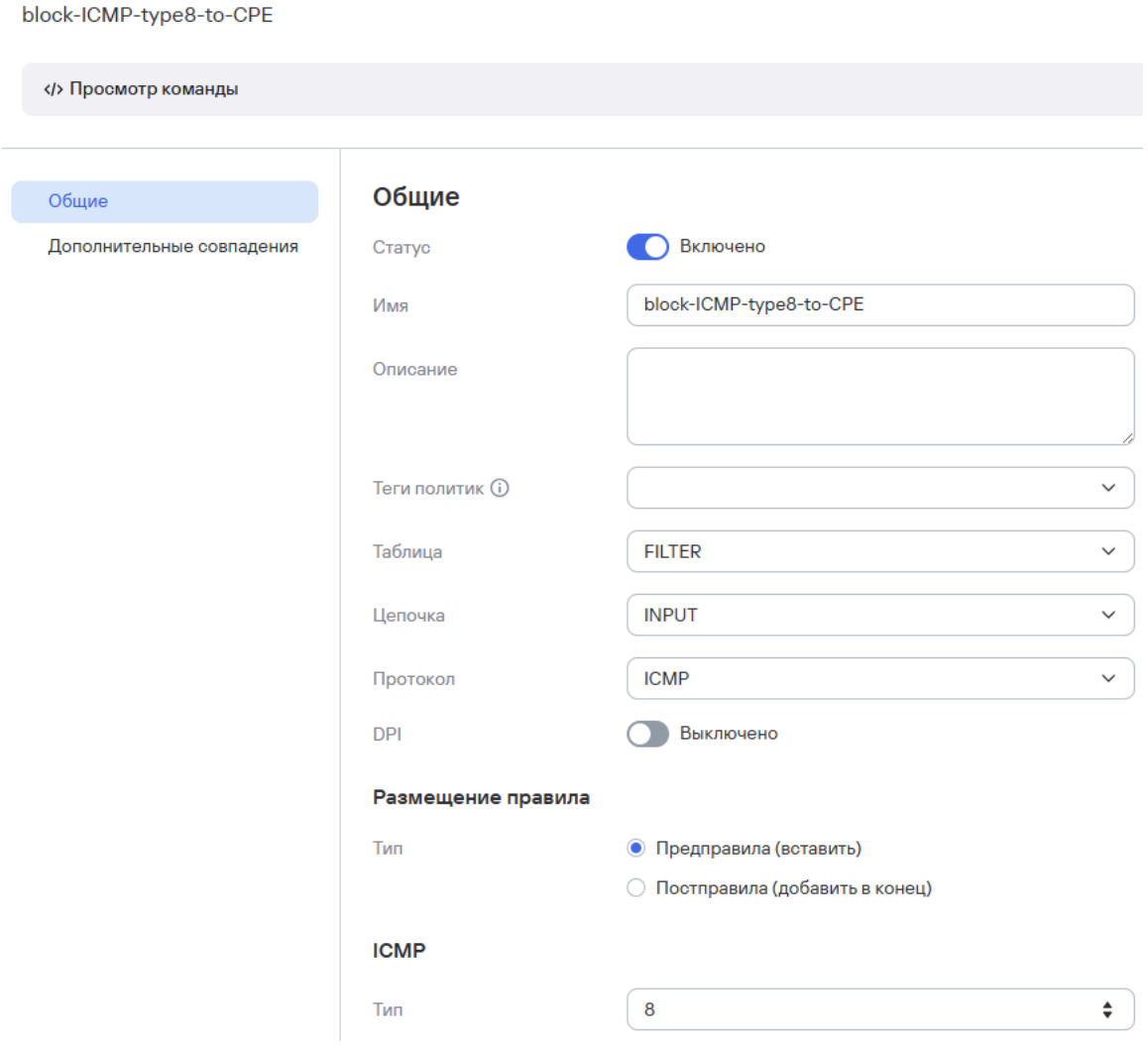
Интерпретация результата:

Traceroute отправляет эхо-запросы ICMP с растущим TTL. Сообщение `ICMP type 11 (Time-Exceeded)` генерируется маршрутизатором, но блокируется расширенным правилом межсетевого экрана, поэтому не появляется в трассировке. После последовательного увеличения хостом A значения TTL оно становится достаточным, чтобы запрос достиг хоста B по адресу `10.123.2.11`, который отвечает обычным сообщением `Echo Reply`. Это единственное сообщение, которое в итоге видно в дампе.

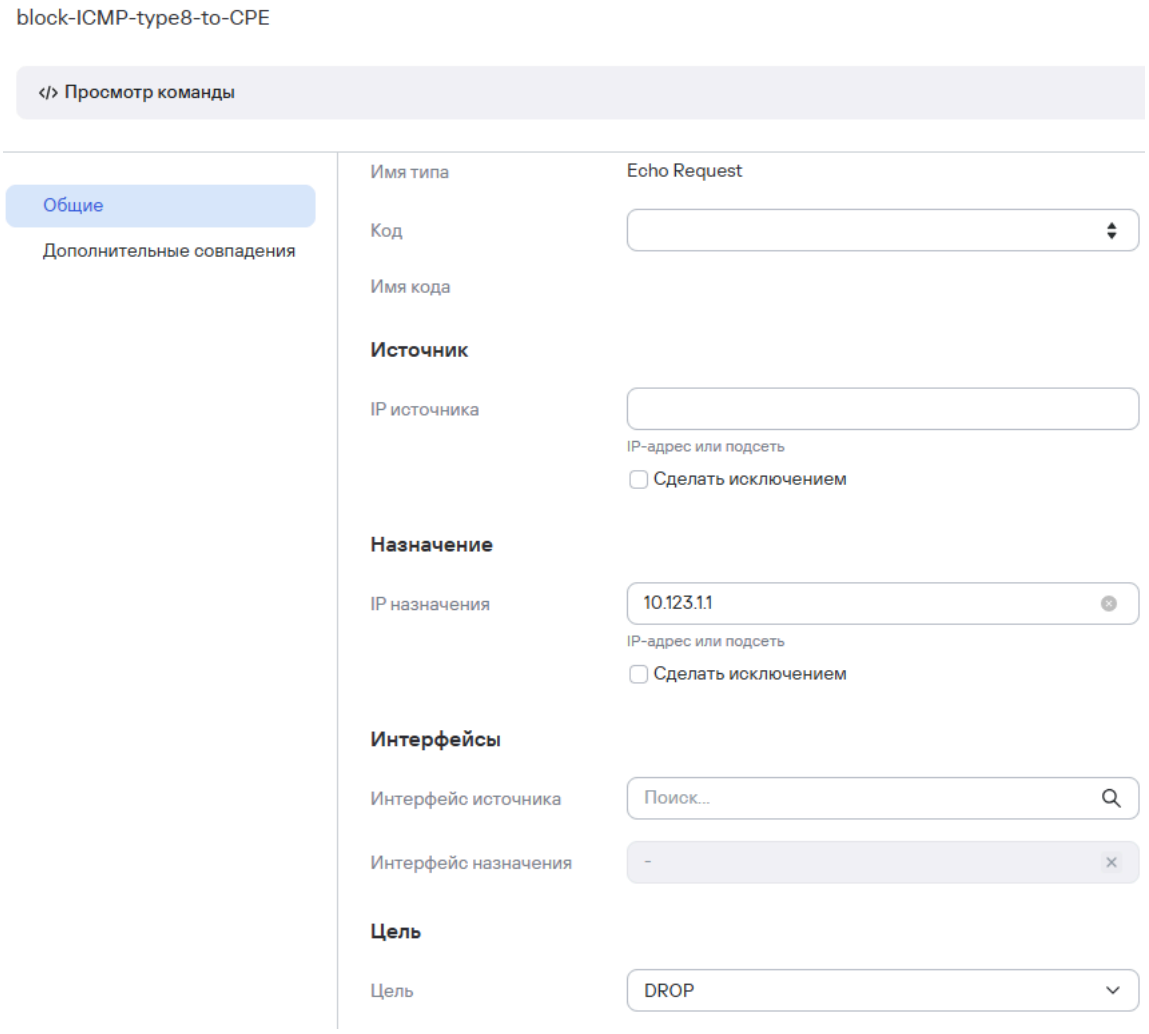
2. Блокировка ответов CPE на ICMP Request

a. Создайте на устройстве CPE расширенное правило, которое отбрасывает ICMP-пакеты,

предназначенные устройству CPE:



Создание расширенного правила для отбрасывания ICMP-пакетов на CPE (1)



Создание расширенного правила для отбрасывания ICMP-пакетов на CPE (2)

Созданное расширенное правило соответствует следующей команде в формате 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"
```

Аналогичное правило в формате iptables при выводе iptables -L выглядит следующим образом:

a. Проверьте работу правила, выполнив на хосте A `ping` до адреса CPE на `eth1`:

```
ping 10.123.1.1
```

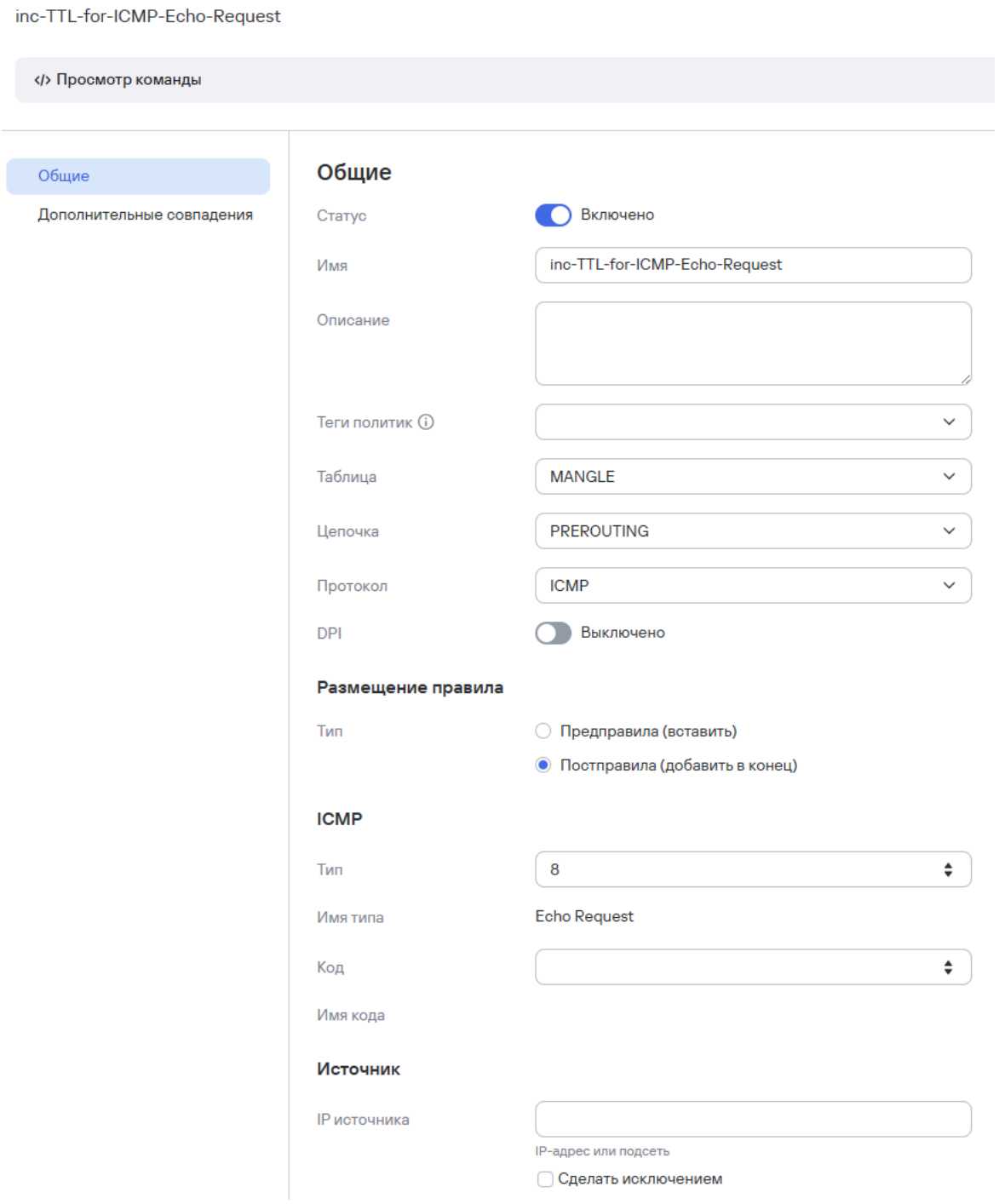
Результат:

```
Request timed out
```

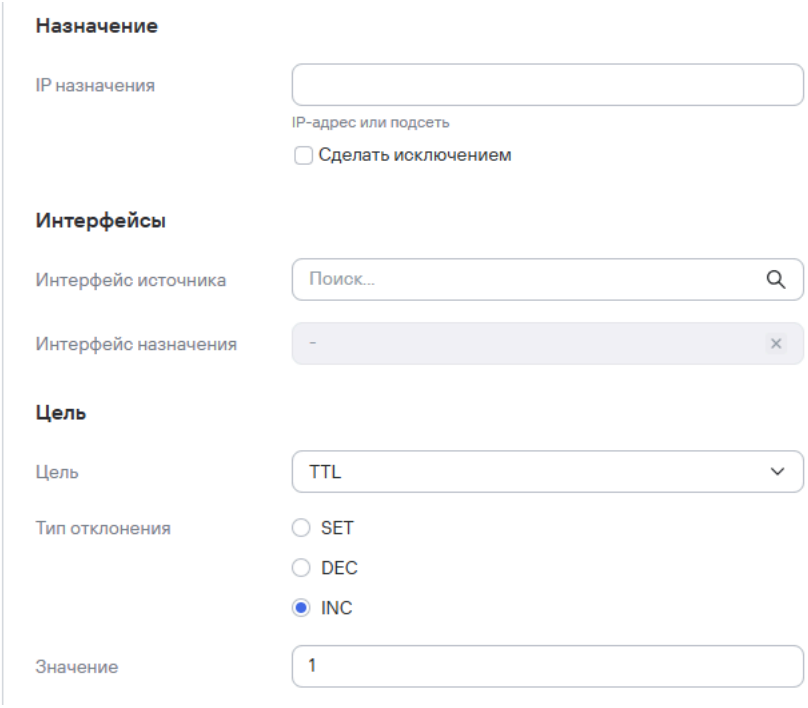
3. Скрытие CPE из пути прохождения трафика с помощью манипуляций с TTL

Вам необходимо создать расширенное правило, которое увеличивает TTL для сообщений `ICMP Type 8 (Echo Request)` на 1 до того, как маршрутизатор уменьшит это значение на 1. Для этого правило необходимо добавить в цепочку PREROUTING таблицы MANGLE.

a. Создайте на устройстве CPE расширенное правило, которое увеличивает TTL на 1:



Создание расширенного правила для увеличения TTL (1)



Создание расширенного правила для увеличения TTL (2)

Созданное расширенное правило соответствует следующей команде в формате 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. Выполняем на Хосте A traceroute до Хоста B.

```
tracert -d 10.123.2.11
```

Результат:

```
1 10.123.2.11
```

Как это правило отражается на трассировке маршрутов между двумя хостами, подключенными к CPE:

Шаг	Что происходит без правила	Что происходит с правилом
1. Хост A отправляет пакет с TTL=1 (первый хоп)	CPE получает пакет, уменьшает TTL до 0, отбрасывает пакет и генерирует ICMP Time-Exceeded (type 11), который возвращается к A. Хост A видит CPE как первый hop.	В цепочке PREROUTING TTL увеличивается до 2. Затем ядро CPE уменьшает его до 1. Пакет не отбрасывается, CPE пересылает его дальше. Поэтому ICMP Time-Exceeded не генерируется и первый хоп (CPE) не появляется в выводе.
2. Пакет поступает на конечный хост (хост B)		Пакет приходит к хосту B с TTL=1. Здесь TTL будет уменьшен до 0 и хост B сгенерирует сообщение ICMP Time-Exceeded. Хост B будет показан как первый хоп в traceroute.
3. Последующие шаги traceroute	На этом шаге TTL увеличивается до 2, CPE снижает его до 1. Хост B снижает TTL до 0, отбрасывает пакет, генерирует сообщение ICMP Time-Exceeded. Хост B будет показан как второй хоп в traceroute.	

Созданное действует только для пакетов `ICMP type 8 (Echo Request)`. Если traceroute или аналогичное средство трассировки маршрутов будет использовать UDP-пакеты, первый хоп все равно будет виден. Чтобы скрыть маршрутизатор от трассировки маршрутов с использованием UDP-пакетов, необходимо создать аналогичное правило для протокола UDP.

4. **Скрытие информации о производителе устройства CPE за счет назначения LAN-интерфейсам устройства MAC-адресов из диапазона LAA**

   Чтобы пользователи локальной сети не смогли получать информацию о производителе устройства CPE через изучение стандартных MAC-адресов его LAN-интерфейсов, вам необходимо переназначить интерфейсам MAC-адреса из диапазона LAA (англ. Locally Administered Address, локально администрируемый адрес). MAC-адрес считается локально администрируемым, если второй наименьший значащий бит (англ. second least significant bit) в его первом октете равняется 1. Пример:

```
06:1A:2B:3C:4D:5E
06 → 0000 0110
```

Чтобы скрыть информации о производителе устройства CPE:

a. Проверьте, что стандартный MAC-адрес устройства CPE содержит информацию о производителе:

1. Выполните `ping` с хоста B на адрес шлюза (интерфейс CPE `eth2` с IP-адресом `10.123.2.1`).

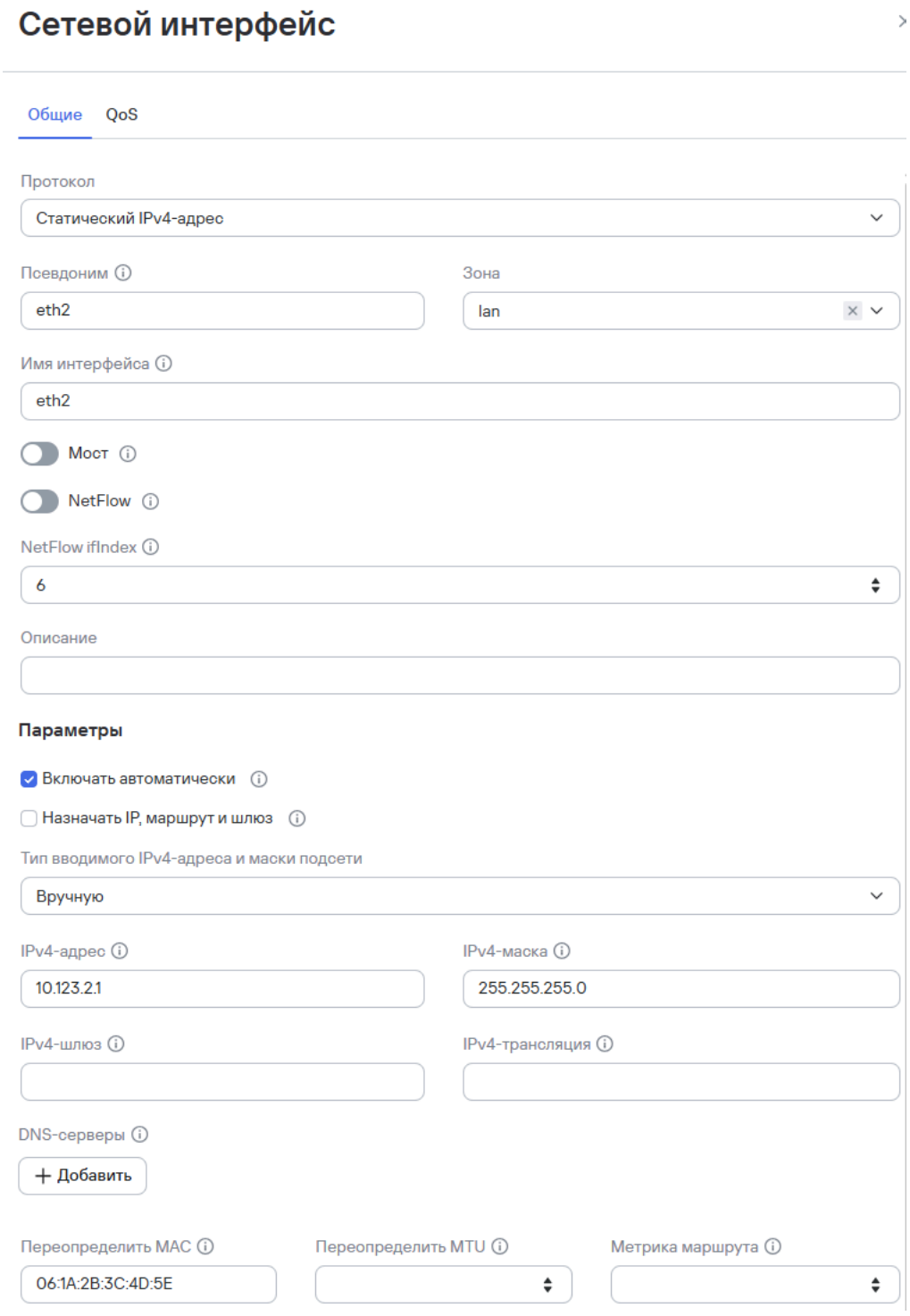
2. Проанализируйте посланный на CPE трафик ICMP с помощью WireShark:

```
> 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)
```

Анализ трафика в Wireshark: для MAC-адреса назначения отображается информация о производителе устройства CPE

В поле `Destination` MAC-адрес интерфейса `eth2` устройства CPE отображается с префиксом производителя `ProxmoxServe_`. Этот префикс соответствует стандартным MAC-адресам, присваиваемым по умолчанию виртуальным машинам в среде виртуализации Proxmox. Благодаря этому можно выяснить, что устройство CPE запущено в виде виртуальной машины в Proxmox. Таким образом, приложение WireShark смогло определить префикс производителя по стандартному MAC-адресу.

a. **Присвойте LAN-интерфейсу устройства CPE в сторону хоста B (`eth2`) MAC-адрес из диапазона LLA:**

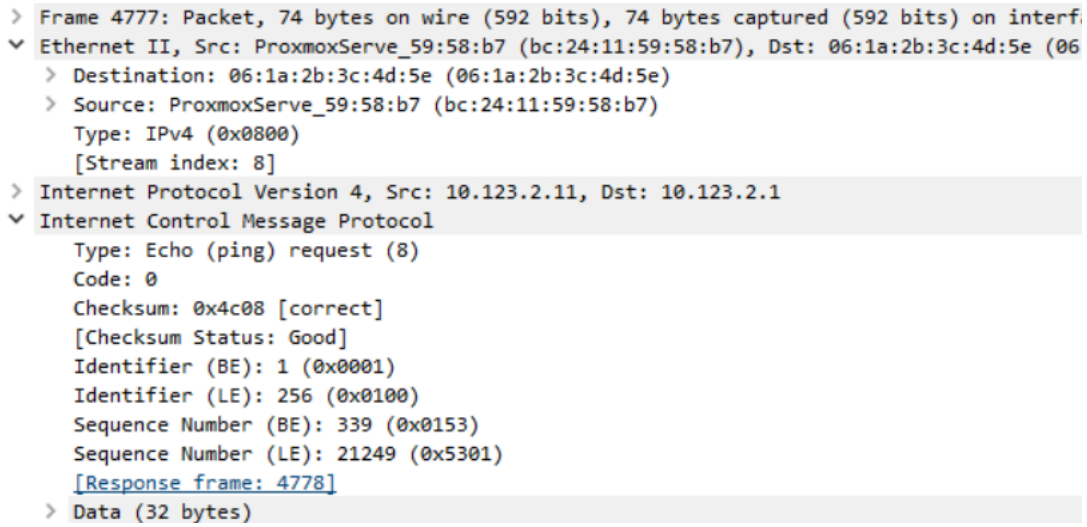


Присвоение LAN-интерфейсу устройства MAC-адреса из диапазона LLA

a. **Убедитесь, что стандартный MAC-адрес устройства CPE не содержит информацию о производителе:**

1. Повторно выполните `ping` с хоста B на адрес шлюза (интерфейс CPE `eth2` с IP-адресом `10.123.2.1`).

2. Проанализируйте посланный на CPE трафик ICMP с помощью WireShark:



Анализ трафика в Wireshark: информация о производителе устройства CPE не отображается

Теперь в поле Destination MAC-адрес интерфейса `eth2` устройства CPE отображается в исходном виде и не указывает на среду виртуализации или производителя сетевого оборудования.

Работа с наборами IP

Вы можете посмотреть таблицу наборов IP в шаблоне межсетевого экрана и на устройстве CPE:

- Для просмотра таблицы наборов IP в шаблоне межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажать на шаблон межсетевого экрана и выбрать вкладку **Наборы IP**.
- Для просмотра таблицы наборов IP на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Межсетевой экран → Наборы IP**.

Информация о наборах IP отображается в следующих столбцах таблицы:

- **Имя** – имя набора IP.
- **Совпадение** – информация о том, относится ли набор IP к источнику или назначению пакетов трафика, а также содержит ли набор IP-адреса или подсети.
- **Записи** – IP-адреса или подсети, которые были добавлены в набор IP.

Создание набора IP

Вы можете создать набор IP в шаблоне межсетевого экрана или на устройстве CPE. Набор IP, созданный в шаблоне межсетевого экрана, автоматически создается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы создать набор IP:

1. Перейдите к созданию набора IP одним из следующих способов:

   - Если вы хотите создать набор IP в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Наборы IP**.

   - Если вы хотите создать набор IP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Наборы IP** и установите флажок **Переопределить**.

   Отобразится таблица наборов IP.

2. Нажмите на кнопку **+ Набор IP**.

3. В открывшемся окне в поле **Имя** введите имя набора IP. Максимальная длина имени: 255 символов.

4. В раскрывающемся списке **Направление** выберите, относится ли набор IP к источнику или назначению пакетов трафика:

   - **Совпадает с источником** – набор IP содержит IP-адреса или подсети источника.

   - **Совпадает с назначением** – набор IP содержит IP-адреса или подсети назначения.

5. В раскрывающемся списке **Тип** выберите, содержит ли набор IP-адреса или подсети.

   - **Набор подсетей** – набор IP содержит подсети.

   - **Набор одиночных IP** – набор IP содержит IP-адреса.

6. Если в раскрывающемся списке **Тип** вы выбрали **Набор подсетей**, укажите подсеть. Для этого в блоке **Список записей** нажмите на кнопку **+ Добавить** и введите IPv4-префикс подести. Вы можете указать диапазоны октетов IPv4-префикса с помощью квадратных скобок, например 192.[165-168].2.0/24.

   Подсеть будет указана и отобразится в блоке **Список записей**. Вы можете указать несколько подсетей и удалить подсети. Для удаления подсети нажмите рядом с ней на значок удаления ✕.

7. Если в раскрывающемся списке **Тип** вы выбрали **Набор одиночных IP**, укажите IP-адрес. Для этого в блоке **Список записей** нажмите на кнопку **+ Добавить** и введите IPv4-адрес. Вы можете указать диапазоны октетов IPv4-адреса с помощью квадратных скобок, например 192.[165-168].2.0.

   IP-адрес будет указан и отобразится в блоке **Список записей**. Вы можете указать несколько IP-адресов и удалить IP-адреса. Для удаления IP-адреса нажмите рядом с ним на значок удаления ✕.

8. Нажмите на кнопку **Создать**.

   Набор IP будет создан и отобразится в таблице.

9. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Выключение и включение набора IP

Вы можете выключить или включить набор IP в шаблоне межсетевого экрана или на устройстве CPE. Набор IP, выключенный или включенный в шаблоне межсетевого экрана, автоматически выключается или включается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы выключить или включить набор IP:

1. Перейдите к выключению или включению набора IP одним из следующих способов:

   - Если вы хотите выключить или включить набор IP в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Наборы IP**.

   - Если вы хотите выключить или включить набор IP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Наборы IP** и установите флажок **Переопределить**.

   Отобразится таблица наборов IP.

2. Нажмите на кнопку **Выключить** или **Включить** рядом с набором IP, который вы хотите выключить или включить.

   Набор IP будет выключен или включен.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Изменение набора IP

Вы можете изменить набор IP в шаблоне межсетевого экрана или на устройстве CPE. Набор IP, измененный в шаблоне межсетевого экрана, автоматически изменяется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы изменить набор IP:

1. Перейдите к изменению набора IP одним из следующих способов:

   - Если вы хотите изменить набор IP в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Наборы IP**.

   - Если вы хотите изменить набор IP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Наборы IP** и установите флажок **Переопределить**.

   Отобразится таблица наборов IP.

2. Нажмите на кнопку **Изменить** рядом с набором IP, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры набора IP. Описание параметров см. в инструкции по созданию набора IP.

4. Нажмите на кнопку **Сохранить**.

   Набор IP будет изменен и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Удаление набора IP

Вы можете удалить набор IP в шаблоне межсетевого экрана или на устройстве CPE. Набор IP, удаленный в шаблоне межсетевого экрана, автоматически удаляется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Удаленные наборы IP невозможно восстановить.

Чтобы удалить набор IP:

1. Перейдите к удалению набора IP одним из следующих способов:

   - Если вы хотите удалить набор IP в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Наборы IP**.

   - Если вы хотите удалить набор IP на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Наборы IP** и установите флажок **Переопределить**.

   Отобразится таблица наборов IP.

2. Нажмите на кнопку **Удалить** рядом с набором IP, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Набор IP будет удален и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с DNAT-правилами

Вы можете посмотреть таблицу DNAT-правил в шаблоне межсетевого экрана и на устройстве CPE:

- Для просмотра таблицы DNAT-правил в шаблоне межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажать на шаблон межсетевого экрана и выбрать вкладку **NAT → DNAT**.

- Для просмотра таблицы DNAT-правил на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Межсетевой экран → NAT → DNAT**.

Информация о DNAT-правилах отображается в следующих столбцах таблицы:

- **Имя** – имя DNAT-правила.
- **Входящий** – критерии, согласно которым межсетевой экран применяет DNAT-правило к пакетам трафика.
- **Перенаправление** – IP-адрес и порт назначения пакетов трафика после применения DNAT-правила.

Создание DNAT-правила

Вы можете создать DNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. DNAT-правило, созданное в шаблоне межсетевого экрана, автоматически создается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы создать DNAT-правило:

1. Перейдите к созданию DNAT-правила одним из следующих способов:

   - Если вы хотите создать DNAT-правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → DNAT**.
   - Если вы хотите создать DNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → DNAT** и установите флажок **Переопределить**.

   Отобразится таблица DNAT-правил.

2. Нажмите на кнопку **+ DNAT**.
3. В открывшемся окне в поле **Имя** введите имя DNAT-правила. Максимальная длина имени: 255 символов.

4. Укажите критерии, согласно которым межсетевой экран применяет DNAT-правило к пакетам трафика:

   a. В раскрывающемся списке **Протокол** выберите протокол пакетов трафика, к которым межсетевой экран применяет DNAT-правило:

      - **IP**.
      - **TCP**.
      - **UDP**.
      - **#** – пользовательский или нестандартный протокол. При выборе этого значения в отобразившемся поле **Номер протокола** введите номер протокола в соответствии со стандартом IANA.

   b. В поле **IP назначения** введите IPv4-адрес или префикс назначения пакетов трафика, к которым межсетевой экран применяет DNAT-правило.

   c. Если вы хотите применять DNAT-правило только к пакетам трафика с указанной зоной межсетевого экрана источника, в раскрывающемся списке **Зона источника** выберите созданную зону межсетевого экрана источника.

   d. Если в раскрывающемся списке **Протокол** вы выбрали **TCP** или **UDP**, и вы хотите применять DNAT-правило только к пакетам трафика с указанным портом назначения, в поле **Порт назначения** введите номер порта назначения. Диапазон значений: от 1 до 65 535.

   e. Если вы хотите применять DNAT-правило только к пакетам трафика с указанным IPv4-адресом или префиксом источника, в поле **IP источника** введите IPv4-адрес или префикс источника.

5. Укажите, как DNAT-правило изменяет пакеты трафика:

   a. В поле **IP назначения** введите новый IPv4-адрес или префикс назначения.

   b. В раскрывающемся списке **Зона назначения** выберите новую зону межсетевого экрана назначения.

   c. Если в раскрывающемся списке **Протокол** вы выбрали **TCP** или **UDP**, и вы хотите изменять номер порта назначения пакетов трафика, в поле **Порт назначения** введите новый номер порта назначения. Диапазон значений: от 1 до 65 535.

6. Нажмите на кнопку **Создать**.

   DNAT-правило будет создано и отобразится в таблице.

7. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Настройка порядка применения DNAT-правил

DNAT-правила применяются к пакетам трафика по порядку, начиная с первого DNAT-правила в верхней части таблицы. По умолчанию DNAT-правила отображаются в таблице в порядке создания. Чем раньше DNAT-правило было создано, тем выше оно отображается в таблице.

Вы можете настроить порядок применения DNAT-правил в шаблоне межсетевого экрана или на устройстве CPE. Порядок применения DNAT-правил, указанный в шаблоне межсетевого экрана, автоматически распространяется на все устройства CPE, которые используют шаблон межсетевого экрана.

Чтобы настроить порядок применения DNAT-правил:

1. Перейдите к настройке порядка применения DNAT-правил одним из следующих способов:

   - Если вы хотите настроить порядок применения DNAT-правил в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → DNAT**.

   - Если вы хотите настроить порядок применения DNAT-правил на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → DNAT** и установите флажок **Переопределить**.

   Отобразится таблица DNAT-правил.

2. Настройте порядок применения DNAT-правил, нажимая рядом с ними на кнопки **Вверх** и **Вниз**.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Выключение и включение DNAT-правила

Вы можете выключить или включить DNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. DNAT-правило, выключенное или включенное в шаблоне межсетевого экрана, автоматически выключается или включается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы выключить или включить DNAT-правило:

1. Перейдите к выключению или включению DNAT-правила одним из следующих способов:

   - Если вы хотите выключить или включить DNAT-правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и в отобразившейся области настройки выберите вкладку **NAT → DNAT**.

   - Если вы хотите выключить или включить DNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, в отобразившейся области настройки выберите вкладку **Межсетевой экран → NAT → DNAT** и установите флажок **Переопределить**.

   Отобразится таблица DNAT-правил.

2. Нажмите на кнопку **Выключить** или **Включить** рядом с DNAT-правилом, которое вы хотите выключить или включить.

   DNAT-правило будет выключено или включено.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Изменение DNAT-правила

Вы можете изменить DNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. DNAT-правило, измененное в шаблоне межсетевого экрана, автоматически изменяется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы изменить DNAT-правило:

1. Перейдите к изменению DNAT-правила одним из следующих способов:

   - Если вы хотите изменить DNAT-правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → DNAT**.

   - Если вы хотите изменить DNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → DNAT** и установите флажок **Переопределить**.

   Отобразится таблица DNAT-правил.

2. Нажмите на кнопку **Изменить** рядом с DNAT-правилом, которое вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры DNAT-правила. Описание параметров см. в инструкции по созданию DNAT-правила.

4. Нажмите на кнопку **Сохранить**.

   DNAT-правило будет изменено и обновится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Удаление DNAT-правила

Вы можете удалить DNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. DNAT-правило, удаленное в шаблоне межсетевого экрана, автоматически удаляется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Удаленные DNAT-правила невозможно восстановить.

Чтобы удалить DNAT-правило:

1. Перейдите к удалению DNAT-правила одним из следующих способов:

   - Если вы хотите удалить DNAT-правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → DNAT**.

   - Если вы хотите удалить DNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → DNAT** и установите флажок **Переопределить**.

   Отобразится таблица DNAT-правил.

2. Нажмите на кнопку **Удалить** рядом с DNAT-правилом, которое вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   DNAT-правило будет удалено и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с SNAT-правилами

Вы можете посмотреть таблицу SNAT-правил в шаблоне межсетевого экрана и на устройстве CPE:

- Для просмотра таблицы SNAT-правил в шаблоне межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажать на шаблон межсетевого экрана и выбрать вкладку **NAT → SNAT**.

- Для просмотра таблицы SNAT-правил на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE, выбрать вкладку **Межсетевой экран → NAT → SNAT** и установить флажок **Переопределить**.

Информация об SNAT-правилах отображается в следующих столбцах таблицы:

- **Имя** – имя SNAT-правила.

- **Исходящий** – критерии, согласно которым межсетевой экран применяет SNAT-правило к пакетам трафика.

- **Действие** – действие, которое SNAT-правило выполняет с пакетами трафика.

Создание SNAT-правила

Вы можете создать SNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. SNAT-правило, созданное в шаблоне межсетевого экрана, автоматически создается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы создать SNAT-правило:

1. Перейдите к созданию SNAT-правила одним из следующих способов:

   - Если вы хотите создать SNAT-правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → SNAT**.

   - Если вы хотите создать SNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → SNAT** и установите флажок **Переопределить**.

   Отобразится таблица SNAT-правил.

2. Нажмите на кнопку **+ SNAT**.

3. В открывшемся окне в поле **Имя** введите имя SNAT-правила. Максимальная длина имени: 255 символов.

4. Укажите критерии, согласно которым межсетевой экран применяет SNAT-правило к пакетам трафика:

   a. В раскрывающемся списке **Протокол** выберите протокол пакетов трафика, к которым межсетевой экран применяет SNAT-правило:

      - **TCP**.
      - **UDP**.
      - **IP**.

   b. В раскрывающемся списке **Зона назначения** выберите созданную зону межсетевого экрана назначения пакетов трафика, к которым межсетевой экран применяет SNAT-правило.

   c. Если вы хотите применять SNAT-правило только к пакетам трафика с указанным IPv4-адресом или префиксом источника, в поле **IP источника** введите IPv4-адрес или префикс источника.

   d. Если вы хотите применять SNAT-правило только к пакетам трафика с указанным IPv4-адресом или префиксом назначения, в поле **IP назначения** введите IPv4-адрес или префикс назначения.

5. В раскрывающемся списке **Действие** выберите **SNAT**.

6. В поле **SNAT IP** введите новый IP-адрес или префикс источника, который SNAT-правило указывает для пакетов трафика.

7. Нажмите на кнопку **Создать**.

   SNAT-правило будет создано и отобразится в таблице.

8. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Настройка порядка применения SNAT-правил

SNAT-правила применяются к пакетам трафика по порядку, начиная с первого SNAT-правила в верхней части таблицы. По умолчанию SNAT-правила отображаются в таблице в порядке создания. Чем раньше SNAT-правило было создано, тем выше оно отображается в таблице.

Вы можете настроить порядок применения SNAT-правил в шаблоне межсетевого экрана или на устройстве CPE. Порядок применения SNAT-правил, указанный в шаблоне межсетевого экрана, автоматически распространяется на все устройства CPE, которые используют шаблон межсетевого экрана.

Чтобы настроить порядок применения SNAT-правил:

1. Перейдите к настройке порядка применения SNAT-правил одним из следующих способов:

   - Если вы хотите настроить порядок применения SNAT-правил в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → SNAT**.

   - Если вы хотите настроить порядок применения SNAT-правил на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → SNAT** и установите флажок **Переопределить**.

   Отобразится таблица SNAT-правил.

2. Настройте порядок применения SNAT-правил, нажимая рядом с ними на кнопки **Вверх** и **Вниз**.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Выключение и включение SNAT-правила

Вы можете выключить или включить SNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. SNAT-правило, выключенное или включенное в шаблоне межсетевого экрана, автоматически выключается или включается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы выключить или включить SNAT-правило:

1. Перейдите к выключению или включению SNAT-правила одним из следующих способов:

   - Если вы хотите выключить или включить SNAT-правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → SNAT**.

   - Если вы хотите выключить или включить SNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → SNAT** и установите флажок **Переопределить**.

   Отобразится таблица SNAT-правил.

2. Нажмите на кнопку **Выключить** или **Включить** рядом со SNAT-правилом, которое вы хотите выключить или включить.

   SNAT-правило будет выключено или включено.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Изменение SNAT-правила

Вы можете изменить SNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. SNAT-правило, измененное в шаблоне межсетевого экрана, автоматически изменяется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы изменить SNAT-правило:

1. Перейдите к изменению SNAT-правила одним из следующих способов:

   - Если вы хотите изменить SNAT-правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → SNAT**.

   - Если вы хотите изменить SNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → SNAT** и установите флажок **Переопределить**.

   Отобразится таблица SNAT-правил.

2. Нажмите на кнопку **Изменить** рядом со SNAT-правилом, которое вы хотите изменить.

3. В отобразившемся окне при необходимости измените параметры SNAT-правила. Описание параметров см. в инструкции по созданию SNAT-правила.

4. Нажмите на кнопку **Сохранить**.

   SNAT-правило будет изменено и отобразится в таблице.

5. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Удаление SNAT-правила

Вы можете удалить SNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. SNAT-правило, удаленное в шаблоне межсетевого экрана, автоматически удаляется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Удаленные SNAT-правила невозможно восстановить.

Чтобы удалить SNAT-правило:

1. Перейдите к удалению SNAT-правила одним из следующих способов:

   - Если вы хотите удалить SNAT-правило в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **NAT → SNAT**.

   - Если вы хотите удалить SNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → NAT → SNAT** и установите флажок **Переопределить**.

   Отобразится таблица SNAT-правил.

2. Нажмите на кнопку **Удалить** рядом со SNAT-правилом, которое вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   SNAT-правило будет удалено и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с передачами

Вы можете посмотреть таблицу передач в шаблоне межсетевого экрана и на устройстве CPE:

- Для просмотра таблицы передач в шаблоне межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажать на шаблон межсетевого экрана и выбрать вкладку **Передачи между зонами**.
- Для просмотра таблицы передач на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE, выбрать вкладку **Межсетевой экран → Передачи между зонами**.

Информация о передачах отображается в следующих столбцах таблицы:

- **От** – исходящая зона межсетевого экрана.
- **До** – входящая зона межсетевого экрана.

Создание передачи

Вы можете создать передачу в шаблоне межсетевого экрана или на устройстве CPE. Передача, созданная в шаблоне межсетевого экрана, автоматически создается на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Чтобы создать передачу:

1. Перейдите к созданию передачи одним из следующих способов:

   - Если вы хотите создать передачу в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Передачи между зонами**.
   - Если вы хотите создать передачу на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Передачи между зонами** и установите флажок **Переопределить**.

   Отобразится таблица передач.

2. Нажмите на кнопку **+ Передача**.
3. В открывшемся окне в раскрывающемся списке **От** выберите созданную исходящую зону межсетевого экрана.
4. В раскрывающемся списке **До** выберите созданную входящую зону межсетевого экрана.

5. Нажмите на кнопку **Создать**.

   Передача будет создана и отобразится в таблице.

6. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Удаление передачи

Вы можете удалить передачу в шаблоне межсетевого экрана или на устройстве CPE. Передача, удаленная в шаблоне межсетевого экрана, автоматически удаляется на всех устройствах CPE, которые используют шаблон межсетевого экрана.

Удаленные передачи невозможно восстановить.

Чтобы удалить передачу:

1. Перейдите к удалению передачи одним из следующих способов:

   - Если вы хотите удалить передачу в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон межсетевого экрана и выберите вкладку **Передачи между зонами**.

   - Если вы хотите удалить передачу на устройстве CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Межсетевой экран → Передачи между зонами** и установите флажок **Переопределить**.

   Отобразится таблица передач.

2. Нажмите на кнопку **Удалить** рядом с передачей, которую вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Передача будет удалена и перестанет отображаться в таблице.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Изменение шаблона межсетевого экрана устройства CPE

Изменение шаблона межсетевого экрана устройства CPE может привести к потере связи с другими устройствами CPE, а также к потере передаваемых пакетов трафика.

Чтобы изменить шаблон межсетевого экрана устройства CPE:

1. В меню перейдите в раздел **SD-WAN → CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, шаблон межсетевого экрана которого вы хотите изменить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию в меню слева выбран раздел **Конфигурация**, в котором отображается основная информация об устройстве CPE. В этом разделе также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В раскрывающемся списке **Шаблон межсетевого экрана** выберите созданный шаблон межсетевого экрана.

4. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Интеграция с внешними средствами защиты информации

Вы можете интегрировать с Kaspersky SD-WAN внешние средства защиты информации (далее также СЗИ) для внешнего управления расширенными правилами межсетевого экрана с помощью API оркестратора. Для интеграции внешних СЗИ вам необходимо создать локального пользователя со специальной ролью **Ограничен-API-внешних-СЗИ,** полномочия которой ограничены только вызовом отдельных операций API, предназначенных для работы с расширенными правилами межсетевого экрана. Для группового включения/выключения расширенных правил межсетевого экрана предусмотрен механизм тегов политик (policy tags). При создании расширенных правил межсетевого экрана им можно присваивать теги политик и затем включать или выключать одновременно все правила, которым присвоен определенный тег.

Пример использования тегов:
Пользователь создается в шаблоне межсетевого экрана следующие расширенные правила:

1. Запретить доступ из пользовательской подсети к сети продуктивных серверов с тегом "user-subnet-compromised";

2. Разрешить доступ из пользовательской подсети ко всем серверным подсетям.
   Т.к. правило 1 помечено тегом и тег пока не введен в действие, правило 1 будет выключено и пользователям будет разрешен доступ ко всем подсетям с серверами, в том числе продуктивными.
   Затем при обнаружении признаков компрометации каких-либо рабочих мест в пользовательской подсети внешнее средство анализа (например, FortiNet NDR или Kaspersky XDR) вызовет API оркестратора по активации тегов с тегом "user-subnet-compromised".
   Оркестатор включит в политике правило 1 и все устройства CPE, на которые установлена эта политика, включат это правило. В результате доступ пользователей к подсети продуктовых серверов будет запрещен.

Описание API

Обращения к API должны проходить аутентификацию и авторизацию.

Аутентификация происходит в три этапа:

1. Отправить `GET` на `/api/core/users/current`, получить пустой ответ со статусом `200/OK` с заголовком, включающим cookie `CSRF-TOKEN`.

2. Для последующей аутентификации отправить `POST` на `/api/authentication`, в теле запроса передать поля `j_username` (имя пользователя) и `j_password` (пароль пользователя), в заголовке `X-CSRF-TOKEN` передать полученный на прошлом шаге токен.

3. Для дальнейших вызовов API необходимо обновлять CSRF-токен, отправляя `GET` на `/api/core/settings/defpage` и получая `200/OK` с новым значением cookie `CSRF-TOKEN`.

Авторизация выполняется на основе роли учетной записи пользователя **Ограничен-API-внешних-СЗИ**. Пользователи с этой ролью имеет доступ только к операциям API для внешних СЗИ. Пользователи с другими ролями не имеют доступа к этим операциям API.

API для внешних СЗИ включает следующие операции:

Метод	Эндпойнт	Описание
`GET`	`/api/nfv/sdwan/externalTools/rules`	Получить конфигурацию правил межсетевого экрана для шаблона межсетевого экрана или устройства CPE
`POST`	`/api/nfv/sdwan/externalTools/rules`	Создать правило межсетевого экрана из внешней СЗИ
`DELETE`	`/api/nfv/sdwan/externalTools/rules`	Удалить правило межсетевого экрана из внешней СЗИ по имени правила

GET	/api/nfv/sdwan/externalTools/policyTags	Получить все теги политик для текущего тенанта
PUT	/api/nfv/sdwan/externalTools/policyTags	Обновить статус тега политики
POST	/api/nfv/sdwan/externalTools/policyTags	Создать тег политики
DELETE	/api/nfv/sdwan/externalTools/policyTags	Удалить тег политики

Более подробную информациб о методах см. в описании API оркестратора.

Управление сетевыми сервисами и виртуализация сетевых функций

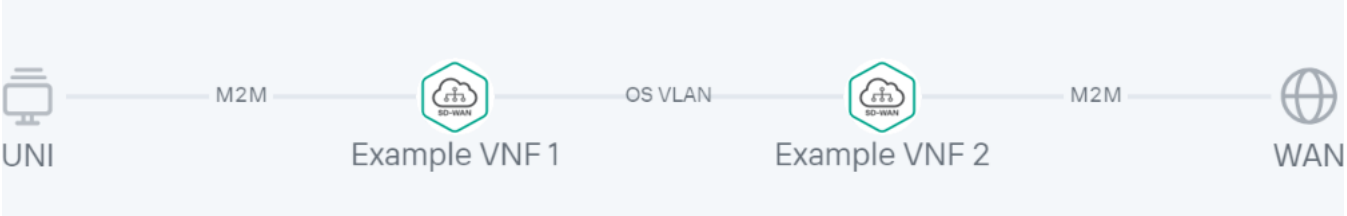
Сетевые сервисы

Сетевые сервисы передают трафик по сети и применяют к трафику сетевые функции, например WAN-оптимизацию, шейпинг и защиту трафика. Каждый сетевой сервис имеет топологию, которую вы строите с помощью графического конструктора. В топологию можно добавить компоненты сетевого сервиса и подключить их друг к другу.

Вы можете построить топологию в шаблоне сетевого сервиса, после назначить шаблон сетевого сервиса тенанту. Вместе с шаблоном сетевого сервиса тенанту автоматически назначаются добавленные в топологию компоненты сетевого сервиса. Тенант может создавать и развертывать сетевые сервисы, при необходимости используя назначенные шаблоны сетевых сервисов, а также изменять сетевые сервисы.

С помощью сетевых сервисов вы можете развертывать экземпляры SD-WAN. Сетевой сервис для развертывания экземпляра SD-WAN называется сетевым сервисом SD-WAN (далее сервис SD-WAN).

Пример построенной топологии сетевого сервиса представлен на рисунке ниже.



Топология сетевого сервиса

Виртуализация сетевых функций

Виртуализация сетевых функций (англ. network function virtualization, далее также NFV) позволяет использовать виртуализированные хранилища, вычислительные ресурсы и сети для предоставления сетевых функций и их объединения в сетевые сервисы.

Вы можете развертывать виртуальные сетевые функции (англ. Virtual Network Functions, далее также VNF) и физические сетевые функции (Physical Network Functions, далее также PNF) в сетевых сервисах. Разница между виртуальными и физическими сетевыми функциями заключается в том, что оркестратор не управляет жизненным циклом физических сетевых функций. Поддерживается использование сетевых функций сторонних производителей.

Kaspersky SD-WAN соответствует архитектуре, указанной в спецификации NFV MANO (NFV Management and Network Orchestration) ETSI, которая представлена следующими основными функциональными компонентами:

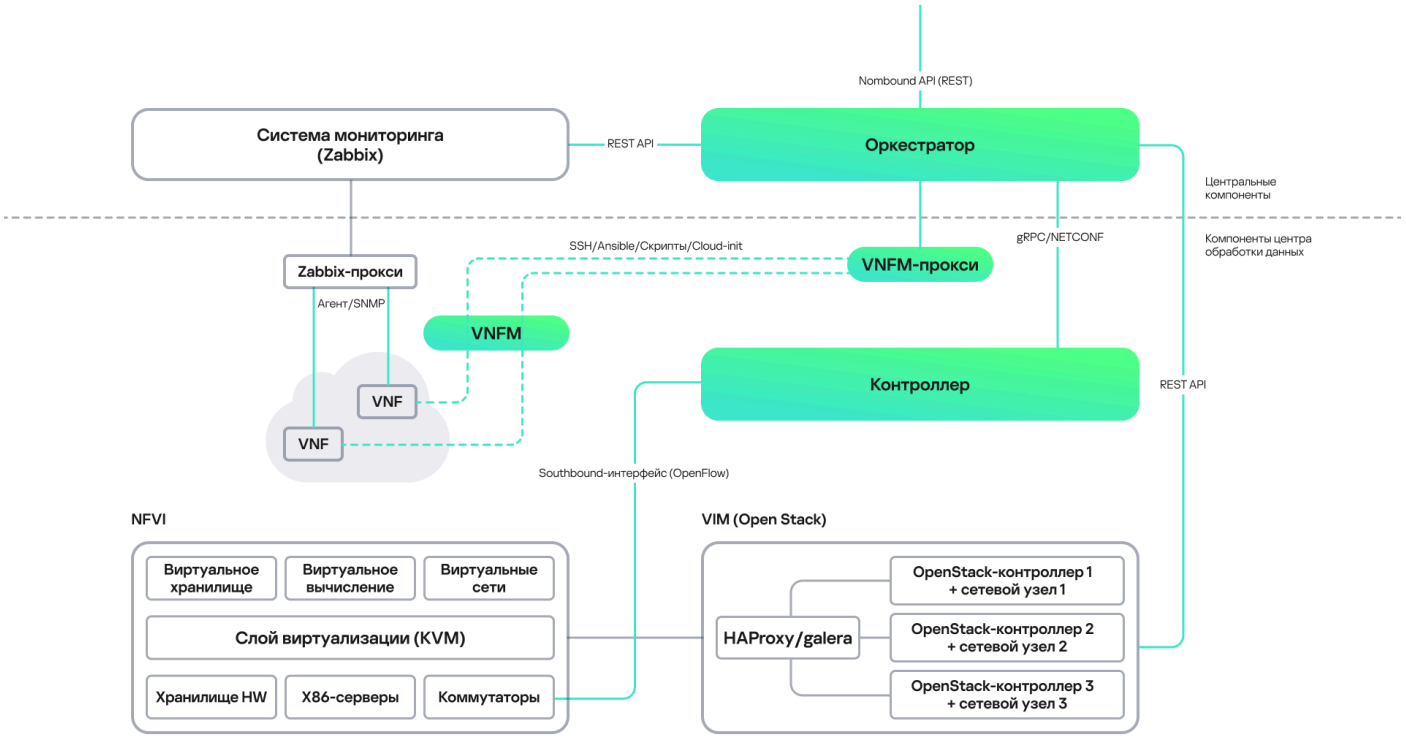
- Оркестратор.
- Менеджер виртуальных сетевых функций (VNFM).
- Менеджер виртуальной инфраструктуры.

- Система мониторинга Zabbix – отслеживает состояние виртуальных сетевых функций и физических сетевых функций и сообщает оркестратору о необходимости восстановить или масштабировать сетевую функцию.

- Инфраструктура NFV – физические ресурсы, такие как аппаратные хранилища, серверы и сетевые устройства.

- Контроллер.

На рисунке ниже показана взаимосвязь между компонентами решения и инфраструктурой NFV. Белым цветом отмечены компоненты внешних решений, зеленым – компоненты Kaspersky SD-WAN, а красными линиями – связи между компонентами.



Инфраструктура NFV

Работа с шаблонами сетевых сервисов

Вы можете посмотреть список шаблонов сетевых сервисов на портале администратора в разделе **Каталог** в панели **Каталог**. Для просмотра информации о доступных компонентах сетевого сервиса вам нужно нажать на значок развертывания ». Отобразятся следующие подразделы:

- **Шаблоны** – таблица шаблонов сетевых сервисов. Информация о шаблонах сетевых сервисов отображается в следующих столбцах таблицы:
  - **Имя** – имя шаблона сетевого сервиса.
  - **Автор** – имя пользователя, который создал шаблон сетевого сервиса.
  - **Создано** – дата и время создания шаблона сетевого сервиса.
  - **Описание** – краткое описание шаблона сетевого сервиса.
- **Общие сетевые сервисы** – список общих сетевых сервисов.
- **Виртуальные сетевые функции** – таблица виртуальных сетевых функций. Информация о виртуальных сетевых функциях отображается в следующих столбцах таблицы:
  - **Имя** – имя виртуальной сетевой функции.
  - **Провайдер** – поставщик виртуальной сетевой функции. Вы можете указать поставщика виртуальной сетевой функции с помощью параметра `provider` в VNF-дескрипторе.
  - **Версия** – версия виртуальной сетевой функции. Вы можете указать версию виртуальной сетевой функции с помощью параметра `version` в VNF-дескрипторе.
  - **Описание** – краткое описание виртуальной сетевой функции. Вы можете указать описание виртуальной сетевой функции с помощью параметра `description` в VNF-дескрипторе.
- **Физические сетевые функции** – таблица физических сетевых функций. Информация о физических сетевых функциях отображается в следующих столбцах таблицы:
  - **Имя** – имя физической сетевой функции.
  - **Провайдер** – поставщик физической сетевой функции. Вы можете указать поставщика физической сетевой функции с помощью параметра `provider` в PNF-дескрипторе.
  - **Версия** – версия физической сетевой функции. Вы можете указать версию физической сетевой функции с помощью параметра `version` в PNF-дескрипторе.
  - **Описание** – краткое описание физической сетевой функции. Вы можете указать описание физической сетевой функции с помощью параметра `description` в PNF-дескрипторе.

Создание шаблона сетевого сервиса

Чтобы создать шаблон сетевого сервиса:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В верхней части страницы нажмите на кнопку **+ Шаблон**.

   Отобразится графический конструктор для построения топологии.

3. Добавьте компоненты сетевого сервиса в топологию:

   a. Перетащите в графический конструктор компоненты сетевого сервиса с панели **Каталог**. В панели отображаются следующие компоненты сетевого сервиса:

      - Шаблоны сетевого сервиса – когда вы добавляете шаблон сетевого сервиса в топологию, топология выстраивается в соответствии с шаблоном сетевого сервиса. Вы можете добавить несколько шаблонов сетевого сервиса в топологию.

      - Общие сетевые сервисы – вам нужно добавить общий сетевой сервис в топологию сетевых сервисов, которые вы хотите подключить к общему сетевому сервису. Вы можете указать краткое описание общего сетевого сервиса.

      - Виртуальные и физические сетевые функции. Действия, которые вы можете выполнить с виртуальными и физическими сетевыми функциями, описаны в разделах Работа с виртуальными сетевыми функциями и Работа с физическими сетевыми функциями.

   b. Перетащите в графический конструктор соединения со вкладки **Соединения**. На вкладке отображаются следующие соединения:

      - **P2P** – транспортный сервис Point-to-Point (далее также P2P-сервис). Вы можете настроить P2P-сервис.

      - **P2M** – транспортный сервис Point-to-Multipoint (далее также P2M-сервис). Вы можете настроить P2M-сервис.

      - **M2M** – транспортный сервис Multipoint-to-Multipoint (далее также M2M-сервис). Вы можете настроить M2M-сервис.

      Остальные соединения относятся к сетевому взаимодействию на уровне VIM и устанавливаются между VNF, хостом которых является облачная платформа OpenStack:

      - **OS shared** – общая сеть, через которую общий сетевой сервис подключается к сетевым сервисам. Вы можете настроить общую сеть.

      - **OS vRouter** – виртуальный маршрутизатор L3. Вы можете настроить виртуальный маршрутизатор.

      - **OS VLAN** – VLAN для передачи тегированного L2-трафика стандарта 802.1Q. Вы можете настроить VLAN.

      - **OS VXLAN** – VXLAN для туннелирования. Вы можете настроить VXLAN.

      - **OS flat** – плоская сеть для передачи нетегированного L2-трафика. Вы можете настроить плоскую сеть.

   c. Выберите вкладку **UNI** и перетащите в графический конструктор UNI устройств CPE. На вкладке отображаются два компонента – **UNI** и **WAN**. Оба компонента обозначают абстрактные UNI, которые тенанту нужно заменить на реальные UNI при создании или изменении сетевого сервиса. Компонент **WAN** используется для обозначения UNI, которые подключаются к WAN.

      Вы можете настроить UNI в топологии.

Компоненты сетевого сервиса будут добавлены в топологию и отобразятся в графическом конструкторе.

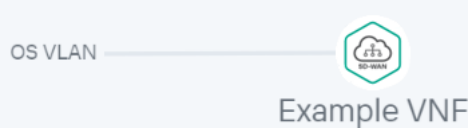
4. Подключите добавленные в топологию компоненты сетевого сервиса друг к другу:

   a. Нажмите на соединение, к которому вы хотите подключить компонент сетевого сервиса.

   b. Нажмите на кнопку **Добавить leaf**, чтобы подключить к соединению компонент сетевого сервиса с ролью leaf. Если вы нажали на P2M-сервис, вы можете нажать на кнопку **Добавить root**, чтобы подключить к соединению компонент сетевого сервиса с ролью root.

   c. Нажмите на компонент сетевого сервиса, который вы хотите подключить к соединению. Если вы нажали на сетевую функцию или общий сетевой сервис, в открывшемся окне выберите порт для подключения соединения.

   К соединению будет подключен компонент сетевого сервиса, и в топологии между ними отобразится линия. Например, на рисунке ниже показана VLAN, к которой подключена виртуальная сетевая функция.



5. Если вы хотите назначить резервные UNI, выполните следующие действия:

   > Резервный UNI можно назначить только для UNI, которые подключены хотя бы к одному соединению.

   a. Нажмите на UNI, для которого вы хотите назначить резервный UNI.

   b. Нажмите на кнопку **Зарезервировать**.

   c. Нажмите на UNI, который вы хотите использовать как резервный.

   UNI будет назначен резервным, и в топологии между UNI, резервным UNI и соединением, к которому подключен UNI, отобразится пунктирная линия. Например, на рисунке ниже WAN является резервным для UNI.



6. Если вы хотите удалить компонент сетевого сервиса из топологии, нажмите на него, после чего нажмите на кнопку **Удалить**.

   Компонент сетевого сервиса будет удален из топологии и перестанет отображаться в графическом конструкторе.

7. Если вы хотите выровнять топологию по горизонтали, нажмите на кнопку **Выровнять**.

8. Если вы хотите, чтобы в топологии не отображались описания добавленных компонентов сетевого сервиса, снимите флажок **Описание**. Этот флажок установлен по умолчанию.

9. В поле **Имя** введите имя шаблона сетевого сервиса.
10. В верхней части графического конструктора нажмите на кнопку **Сохранить**.

    Шаблон сетевого сервиса будет создан и отобразится в панели **Каталог** на вкладке **Шаблоны**.

Изменение шаблона сетевого сервиса

Когда вы изменяете шаблон сетевого сервиса, изменения не применяются к сетевым сервисам, которые уже были созданы и развернуты с помощью шаблона сетевого сервиса.

Чтобы изменить шаблон сетевого сервиса:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.
2. В панели **Каталог** выберите вкладку **Шаблоны**.

   Отобразится список шаблонов сетевого сервиса.
3. Нажмите на шаблон сетевого сервиса, который вы хотите изменить.

   Отобразится графический конструктор для построения топологии.
4. При необходимости измените параметры шаблона сетевого сервиса. Описание параметров см. в инструкции по созданию шаблона сетевого сервиса.
5. В верхней части графического конструктора нажмите на кнопку **Сохранить**.

Шаблон сетевого сервиса будет изменен и обновится в панели **Каталог** на вкладке **Шаблоны**.

Удаление шаблона сетевого сервиса

Удаленные шаблоны сетевых сервисов невозможно восстановить.

Чтобы удалить шаблон сетевого сервиса:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.
2. В панели **Каталог** выберите вкладку **Шаблоны**.

   Отобразится список шаблонов сетевых сервисов.
3. Нажмите на значок удаления ✕ рядом с шаблоном сетевого сервиса, который вы хотите удалить.
4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Шаблон сетевого сервиса будет удален и перестанет отображаться в панели **Каталог** на вкладке **Шаблоны**.

Работа с сетевыми сервисами

Перед началом работы с сетевыми сервисами вам нужно войти на портал самообслуживания тенанта. Вы можете посмотреть список сетевых сервисов в разделе **Каталог** в панели **Сетевые сервисы**. Для просмотра информации о добавленных в топологию сетевого сервиса компонентах вам нужно нажать на сетевой сервис, после чего в панели **Объекты** нажать на значок развертывания ». Отобразятся следующие подразделы:

- **VNF** – таблица виртуальных сетевых функций. Информация о виртуальных сетевых функциях отображается в следующих столбцах таблицы:
  - **Имя** – имя виртуальной сетевой функции.
  - **Провайдер** – поставщик виртуальной сетевой функции. Вы можете указать поставщика виртуальной сетевой функции с помощью параметра `provider` в VNF-дескрипторе.
  - **Версия** – версия виртуальной сетевой функции. Вы можете указать версию виртуальной сетевой функции с помощью параметра `version` в VNF-дескрипторе.
  - **Описание** – краткое описание виртуальной сетевой функции. Вы можете указать описание виртуальной сетевой функции с помощью параметра `description` в VNF-дескрипторе.
  - **Состояние** – состояние виртуальной сетевой функции:
    - **PENDING** – выполняется изменение состояния виртуальной сетевой функции.
    - **UNDEPLOYED** – виртуальная сетевая функция добавлена в топологию сетевого сервиса, но сетевой сервис не развернут.
    - **SCHEDULED** – виртуальная сетевая функция добавлена в топологию сетевого сервиса. Планируется развертывание виртуальной сетевой функции на устройстве uCPE, но отсутствует связь между оркестратором и устройством uCPE. Сетевой сервис будет развернут при восстановлении связи.
    - **TERMINATING** – виртуальная сетевая функция находится в процессе удаления.
    - **RUNNING** – виртуальная сетевая функция работает нормально.
    - **ERROR** – при развертывании сетевого сервиса, в топологию которого добавлена виртуальная сетевая функция, произошла ошибка.
    - **SCALING** – выполняется изменение варианта развертывания виртуальной сетевой функции.
    - **HEALING** – выполняется автоматическое восстановление виртуальной сетевой функции.
    - **DELETED** – виртуальная сетевая функция успешно удалена.
    - **UPDATING** – выполняется изменение сетевого сервиса, в топологию которого добавлена виртуальная сетевая функция.
    - **REPARING** – при изменении сетевого сервиса произошла ошибка и выполняется восстановление предыдущих параметров сетевого сервиса.

- **CHECKING** – выполняется проверка консистентности сетевого сервиса, в который добавлена виртуальная сетевая функция.
- **DEGRADED** – проверка консистентности сетевого сервиса, в который добавлена виртуальная сетевая функция, показала, что виртуальная сетевая функция не консистентна.
- **RECOVERING** – выполняется повторное развертывание виртуальной сетевой функции.

- **Автовосстановление** – информация о том, указаны ли параметры автоматического восстановления VDU в блоке `auto_healing` пакета VNF:
  - **Да**.
  - **Нет**.
- **Автомасштабирование** – информация о том, указаны ли параметры масштабирования виртуальной сетевой функции в блоке `scaling` пакета VNF:
  - **Да**.
  - **Нет**.

- **Физические сетевые функции** – таблица физических сетевых функций. Информация о физических сетевых функциях отображается в следующих столбцах таблицы:
  - **Имя** – имя физической сетевой функции.
  - **Провайдер** – поставщик физической сетевой функции. Вы можете указать поставщика физической сетевой функции с помощью параметра `provider` в PNF-дескрипторе.
  - **Версия** – версия физической сетевой функции. Вы можете указать версию физической сетевой функции с помощью параметра `version` в PNF-дескрипторе.
  - **Описание** – краткое описание физической сетевой функции. Вы можете указать описание физической сетевой функции с помощью параметра `description` в PNF-дескрипторе.
  - **Состояние** – состояние физической сетевой функции:
    - **PENDING** – выполняется изменение состояния физической сетевой функции.
    - **UNDEPLOYED** – физическая сетевая функция добавлена в топологию сетевого сервиса, но сетевой сервис не развернут.
    - **TERMINATING** – физическая сетевая функция находится в процессе удаления.
    - **RUNNING** – физическая сетевая функция работает нормально.
    - **ERROR** – при развертывании сетевого сервиса, в топологию которого добавлена физическая сетевая функция, произошла ошибка.
    - **SCALING** – выполняется изменение варианта развертывания физической сетевой функции.
    - **HEALING** – выполняется автоматическое восстановление физической сетевой функции.
    - **DELETED** – физическая сетевая функция успешно удалена.

- **UPDATING** – выполняется изменение сетевого сервиса, в топологию которого добавлена физическая сетевая функция.
- **REPARING** – при изменении сетевого сервиса произошла ошибка и выполняется восстановление предыдущих параметров сетевого сервиса.
- **CHECKING** – выполняется проверка консистентности сетевого сервиса, в который добавлена физическая сетевая функция.
- **DEGRADED** – проверка консистентности сетевого сервиса, в который добавлена физическая сетевая функция, показала, что физическая сетевая функция не консистентна.
- **RECOVERING** – выполняется повторное развертывание физической сетевой функции.

- **Автовосстановление** – информация о том, указаны ли параметры автоматического восстановления в блоке `auto_healing` пакета PNF:
  - **Да**.
  - **Нет**.
- **Автомасштабирование** – информация о том, указаны ли параметры масштабирования физической сетевой функции в блоке `scaling` пакета PNF:
  - **Да**.
  - **Нет**.

- **Общий сетевой сервис** – список общих сетевых сервисов.

- **Соединения** – таблица соединений. Информация о соединениях отображается в следующих столбцах таблицы:
  - **Имя** – имя соединения.
  - **Тип** – тип соединения.
  - **Статус** – статус соединения:
    - **NONE** – проверка консистентности сетевого сервиса, в который добавлено соединение, показала, что соединение не существует.
    - **OK** – проверка консистентности сетевого сервиса, в который добавлено соединение, показала, что соединение существует.
  - **Общий** – информация о том, используется ли соединение для создания общего сетевого сервиса:
    - **Да**.
    - **Нет**.
- **UNI** – таблица UNI. Информация о UNI отображается в следующих столбцах таблицы:
  - **Имя** – имя UNI.
  - **Псевдоним** – имя UNI в момент добавления в топологию сетевого сервиса.
  - **Статус** – статус UNI:
    - **NONE** – проверка консистентности сетевого сервиса, в который добавлен UNI, показала, что UNI не существует.
    - **OK** – проверка консистентности сетевого сервиса, в который добавлен UNI, показала, что UNI существует.

Создание сетевого сервиса

Чтобы создать сетевой сервис:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В верхней части панели **Сетевые сервисы** нажмите на кнопку **+ Сетевой сервис**.

   Отобразится графический конструктор для построения топологии.

3. Добавьте компоненты сетевого сервиса в топологию:

   a. Перетащите в графический конструктор компоненты сетевого сервиса с панели **Каталог**. В панели отображаются следующие компоненты сетевого сервиса:

      - Шаблоны сетевого сервиса – когда вы добавляете шаблон сетевого сервиса в топологию, топология выстраивается в соответствии с шаблоном сетевого сервиса. Вы можете добавить несколько шаблонов сетевого сервиса в топологию.

      - Общие сетевые сервисы – вам нужно добавить общий сетевой сервис в топологию сетевых сервисов, которые вы хотите подключить к общему сетевому сервису. Вы можете указать краткое описание общего сетевого сервиса.

      - Виртуальные и физические сетевые функции. Действия, которые вы можете выполнить с виртуальными и физическими сетевыми функциями, описаны в разделах Работа с виртуальными сетевыми функциями и Работа с физическими сетевыми функциями.

   b. Перетащите в графический конструктор соединения со вкладки **Соединения**. На вкладке отображаются следующие соединения:

      - **P2P** – транспортный сервис Point-to-Point (далее также P2P-сервис). Вы можете настроить P2P-сервис.

      - **P2M** – транспортный сервис Point-to-Multipoint (далее также P2M-сервис). Вы можете настроить P2M-сервис.

      - **M2M** – транспортный сервис Multipoint-to-Multipoint (далее также M2M-сервис). Вы можете настроить M2M-сервис.

      Остальные соединения относятся к сетевому взаимодействию на уровне VIM и устанавливаются между VNF, хостом которых является облачная платформа OpenStack:

      - **OS shared** – общая сеть, через которую общий сетевой сервис подключается к сетевым сервисам. Вы можете настроить общую сеть.

      - **OS vRouter** – виртуальный маршрутизатор L3. Вы можете настроить виртуальный маршрутизатор.

      - **OS VLAN** – VLAN для передачи тегированного L2-трафика стандарта 802.1Q. Вы можете настроить VLAN.

      - **OS VXLAN** – VXLAN для туннелирования. Вы можете настроить VXLAN.

      - **OS flat** – плоская сеть для передачи нетегированного L2-трафика. Вы можете настроить плоскую сеть.

   c. Выберите вкладку **UNI** и перетащите в графический конструктор UNI устройств CPE. Если вы используете шаблон сетевого сервиса, вам нужно заменить абстрактные UNI в топологии на реальные UNI. Абстрактные UNI могут быть обозначены двумя компонентами – **UNI** и **WAN**. Компонент **WAN** используется для обозначения UNI, которые подключаются к WAN.

      Вы можете настроить UNI.

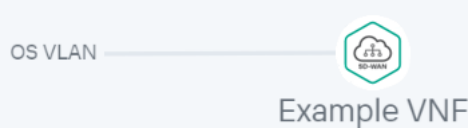
4. Подключите добавленные в топологию компоненты сетевого сервиса друг к другу:

   a. Нажмите на соединение, к которому вы хотите подключить компонент сетевого сервиса.

   b. Нажмите на кнопку **Добавить leaf**, чтобы подключить к соединению компонент сетевого сервиса с ролью leaf. Если вы нажали на P2M-сервис, вы можете нажать на кнопку **Добавить root**, чтобы подключить к соединению компонент сетевого сервиса с ролью root.

   c. Нажмите на компонент сетевого сервиса, который вы хотите подключить к соединению. Если вы нажали на сетевую функцию или общий сетевой сервис, в открывшемся окне выберите порт для подключения соединения.

   К соединению будет подключен компонент сетевого сервиса, и в топологии между ними отобразится линия. Например, на рисунке ниже показана VLAN, к которой подключена виртуальная сетевая функция.



5. Если вы хотите назначить резервные UNI, выполните следующие действия:

   > Резервный UNI можно назначить только для UNI, которые подключены хотя бы к одному соединению.

   a. Нажмите на UNI, для которого вы хотите назначить резервный UNI.

   b. Нажмите на кнопку **Зарезервировать**.

   c. Нажмите на UNI, который вы хотите использовать как резервный.

   UNI будет назначен резервным, и в топологии между UNI, резервным UNI и соединением, к которому подключен UNI, отобразится пунктирная линия. Например, на рисунке ниже WAN является резервным для UNI.



6. Если вы хотите удалить компонент сетевого сервиса из топологии, нажмите на него, после чего нажмите на кнопку **Удалить**.

   Компонент сетевого сервиса будет удален из топологии и перестанет отображаться в графическом конструкторе.

7. Если вы хотите выровнять топологию по горизонтали, нажмите на кнопку **Выровнять**.

8. Если вы хотите, чтобы в топологии не отображались описания добавленных компонентов сетевого сервиса, снимите флажок **Описание**. Этот флажок установлен по умолчанию.

9. В поле **Имя** введите имя сетевого сервиса.

10. Завершите создание сетевого сервиса одним из следующих способов:

    - Если вы хотите сохранить сетевой сервис, нажмите на кнопку **Сохранить**.
    - Если вы хотите сохранить и развернуть сетевой сервис, нажмите на кнопку **Развернуть**.

Сетевой сервис будет создан и отобразится в панели **Сетевые сервисы**. Если вы нажали на кнопку **Развернуть**, начнется развертывание сетевого сервиса, которое может длиться несколько минут. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

Изменение сетевого сервиса

Чтобы изменить сетевой сервис:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис, который вы хотите изменить.

   Отобразится графический конструктор для построения топологии.

3. В верхней части графического конструктора нажмите на кнопку **Изменить**.

4. При необходимости измените параметры сетевого сервиса. Описание параметров см. в инструкции по созданию сетевого сервиса.

5. Завершите изменение сетевого сервиса одним из следующих способов:

   - При изменении не развернутого сетевого сервиса выполните одно из следующих действий:
     - Если вы хотите сохранить сетевой сервис, нажмите на кнопку **Сохранить**.
     - Если вы хотите сохранить и развернуть сетевой сервис, нажмите на кнопку **Развернуть**.
   - При изменении развернутого сетевого сервиса нажмите на кнопку **Развернуть изменения**, чтобы развернуть измененный сетевой сервис.

Сетевой сервис будет изменен и обновится в панели **Сетевые сервисы**. Если вы нажали на кнопку **Развернуть** или **Развернуть изменения**, начнется развертывание, которое может длиться несколько минут. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

Развертывание сетевого сервиса

Если в топологию сетевого сервиса добавлена виртуальная сетевая функция, развернутая на устройстве uCPE и отсутствует связь между оркестратором и устройством uCPE, развертывание сетевого сервиса будет выполнено при восстановлении связи.

Чтобы развернуть сетевой сервис:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис, который вы хотите развернуть.

   Отобразится графический конструктор для построения топологии.

3. В верхней части графического конструктора нажмите на кнопку **Изменить**.

4. Нажмите на кнопку **Развернуть**.

Начнется развертывание сетевого сервиса, которое может длиться несколько минут. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

Проверка консистентности сетевого сервиса

Проверка консистентности (англ. consistency check) позволяет проверить, существуют ли добавленные в топологию компоненты сетевого сервиса.

Чтобы проверить консистентность сетевого сервиса:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на значок настройки ⚙ → **Проверить консистентность** рядом с сетевым сервисом, консистентность которого вы хотите проверить.

3. В открывшемся окне подтверждения нажмите на кнопку **Подтвердить**.

Начнется проверка консистентности сетевого сервиса.

Повторное развертывание сетевого сервиса

Повторное развертывание сетевого сервиса может привести к краткосрочным перебоям в его работе или временной потери работоспособности. Мы рекомендуем планировать работы по повторному развертыванию в соответствии с требованиями вашей организации, чтобы свести нарушения работы к минимуму.

Чтобы повторно развернуть сетевой сервис:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на значок настройки ⚙ → **Повторно развернуть** рядом с сетевым сервисом, который вы хотите повторно развернуть.

3. В открывшемся окне подтверждения нажмите на кнопку **Подтвердить**.

Начнется повторное развертывание сетевого сервиса, которое может длиться несколько минут. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

Выключение и включение автоматического восстановления сетевого сервиса

Zabbix-сервер обеспечивает мониторинг компонентов сетевого сервиса и при обнаружении проблемы отправляет REST API-запрос оркестратору. Если функция автоматического восстановления сетевого сервиса включена, оркестратор начинает автоматическое восстановление компонентов сетевого сервиса, с которыми возникли проблемы. По умолчанию функция включена.

Чтобы выключить или включить автоматическое восстановление сетевого сервиса:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на значок настройки ⚙ → **Выключить автовосстановление** или **Включить автовосстановление** рядом с сетевым сервисом, автоматическое восстановление которого вы хотите выключить или включить.

Автоматическое восстановление сетевого сервиса будет выключено или включено.

Вы можете выполнить автоматическое восстановление виртуальных сетевых функций или входящих в их состав VDU, даже если для сетевого сервиса выключено автоматическое восстановление.

Просмотр журнала работы сетевого сервиса

Чтобы посмотреть журнал работы сетевого сервиса:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на значок настройки ⚙ → **Открыть журнал** рядом с сетевым сервисом, журнал работы которого вы хотите посмотреть.

Откроется страница с журналом работы сетевого сервиса.

Удаление сетевого сервиса

Удаленные сетевые сервисы невозможно восстановить.

Чтобы удалить сетевой сервис:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на значок настройки ⚙ → **Удалить** рядом с сетевым сервисом, который вы хотите удалить.

3. В отобразившемся окне подтверждения нажмите на кнопку **Удалить**.

Сетевой сервис будет удален и перестанет отображаться в панели **Сетевые сервисы**.

Сценарий: развертывание виртуальной сетевой функции

Вы можете развернуть виртуальную сетевую функцию для тенанта в сетевом сервисе. Жизненным циклом виртуальных сетевых функций управляет оркестратор. Для развертывания виртуальных сетевых функций требуется наличие облачной платформы OpenStack.

Например, вы можете развернуть в центральном офисе вашей организации виртуальную сетевую функцию для защиты пользовательского трафика, который передается между устройствами CPE.

Сценарий развертывания виртуальной сетевой функции состоит из следующих этапов:

1. **Подготовка пакета VNF**

   Подготовьте пакет VNF, которую вы хотите развернуть, после чего загрузите пакет VNF в веб-интерфейс оркестратора. При необходимости перед загрузкой пакета VNF в веб-интерфейс оркестратора вы можете включить защиту пакетов VNF и PNF от подмены.

2. **Обеспечение сетевой связности между оркестратором и облачной платформой OpenStack**

   Обеспечьте сетевую связность между виртуальной машиной или физическим сервером, на котором развернут оркестратор, и облачной платформой OpenStack.

3. **Назначение виртуальной сетевой функции тенанту**

   Назначьте виртуальную сетевую функцию тенанту, для которого вы хотите развернуть виртуальную сетевую функцию, одним из следующих способов:

   - Если вы хотите развернуть виртуальную сетевую функцию с помощью шаблона сетевого сервиса, выполните следующие действия:

     1. Добавьте виртуальную сетевую функцию в топологию при создании или изменении шаблона сетевого сервиса.

     2. При необходимости настройте топологию и виртуальную сетевую функцию. Действия, которые вы можете выполнить с виртуальными сетевыми функциями, описаны в разделе Работа с виртуальными сетевыми функциями.

     3. Назначьте шаблон сетевого сервиса тенанту.

   - Если вы хотите развернуть виртуальную сетевую функцию без шаблона сетевого сервиса, назначьте виртуальную сетевую функцию тенанту.

4. **Вход на портал самообслуживания тенанта**

   Войдите на портал самообслуживания тенанта.

5. **Развертывание виртуальной сетевой функции**

   Выполните следующие действия:

   1. Добавьте виртуальную сетевую функцию в топологию при создании или изменении сетевого сервиса одним из следующих способов:

      - Если вы хотите развернуть виртуальную сетевую функцию с помощью шаблона сетевого сервиса, добавьте шаблон сетевого сервиса в топологию.
      - Если вы хотите развернуть виртуальную сетевую функцию без шаблона сетевого сервиса, добавьте виртуальную сетевую функцию в топологию.

   2. При необходимости настройте топологию и виртуальную сетевую функцию. Действия, которые вы можете выполнить с виртуальными сетевыми функциями, описаны в разделе Работа с виртуальными сетевыми функциями.

   3. Разверните виртуальную сетевую функцию одним из следующих способов:

      - Если вы добавили виртуальную сетевую функцию в топологию при создании сетевого сервиса, разверните сетевой сервис.
      - Если вы добавили виртуальную сетевую функцию в топологию при изменении сетевого сервиса, разверните измененный сетевой сервис.

Виртуальная сетевая функция будет развернута.

Сценарий: развертывание физической сетевой функции

Вы можете развернуть физическую сетевую функцию для тенанта в сетевом сервисе. В качестве физических сетевых функций можно использовать специализированное оборудование или виртуальные сущности, созданные с помощью сторонних сред виртуализации. Оркестратор не управляет жизненным циклом физических сетевых функций.

Например, вы можете развернуть в центральном офисе вашей организации физическую сетевую функцию для защиты пользовательского трафика, который передается между устройствами CPE.

Сценарий развертывания физической сетевой функции состоит из следующих этапов:

1. **Подготовка пакета PNF**

   Подготовьте пакет PNF, которую вы хотите развернуть, после чего загрузите пакет PNF в веб-интерфейс оркестратора. При необходимости перед загрузкой пакета PNF в веб-интерфейс оркестратора вы можете включить защиту пакетов VNF и PNF от подмены.

2. **Обеспечение сетевой связности между оркестратором и физической сетевой функцией**

   Обеспечьте сетевую связность между виртуальной машиной или физическим сервером, на котором развернут оркестратор, и специализированным оборудованием или виртуальной сущностью для развертывания физической сетевой функции.

3. **Назначение физической сетевой функции тенанту**

   Назначьте физическую сетевую функцию тенанту, для которого вы хотите развернуть физическую сетевую функцию, одним из следующих способов:

   - Если вы хотите развернуть физическую сетевую функцию с помощью шаблона сетевого сервиса, выполните следующие действия:

     1. Добавьте физическую сетевую функцию в топологию при создании или изменении шаблона сетевого сервиса.
     2. При необходимости настройте топологию и физическую сетевую функцию. Действия, которые вы можете выполнить с физическими сетевыми функциями, описаны в разделе Работа с физическими сетевыми функциями.
     3. Назначьте шаблон сетевого сервиса тенанту.

   - Если вы хотите развернуть физическую сетевую функцию без шаблона сетевого сервиса, назначьте физическую сетевую функцию тенанту.

4. **Вход на портал самообслуживания тенанта**

   Войдите на портал самообслуживания тенанта.

5. **Развертывание физической сетевой функции**

   Выполните следующие действия:

   1. Добавьте физическую сетевую функцию в топологию при создании или изменении сетевого сервиса одним из следующих способов:

      - Если вы хотите развернуть физическую сетевую функцию с помощью шаблона сетевого сервиса, добавьте шаблон сетевого сервиса в топологию.
      - Если вы хотите развернуть физическую сетевую функцию без шаблона сетевого сервиса, добавьте физическую сетевую функцию в топологию.

   2. При необходимости настройте топологию и физическую сетевую функцию. Действия, которые вы можете выполнить с физическими сетевыми функциями, описаны в разделе Работа с физическими сетевыми функциями.
   3. Разверните физическую сетевую функцию одним из следующих способов:

      - Если вы добавили физическую сетевую функцию в топологию при создании сетевого сервиса, разверните сетевой сервис.
      - Если вы добавили физическую сетевую функцию в топологию при изменении сетевого сервиса, разверните измененный сетевой сервис.

Физическая сетевая функция будет развернута.

Работа с пакетами VNF и PNF

Пакет VNF и *PNF* – это ZIP-архив, в которой вам нужно поместить следующие компоненты для развертывания и управления жизненным циклом сетевой функции:

- VNF/PNF-дескриптор – файл с параметрами сетевой функции.
- /image – образы виртуальных машин в формате QCOW для развертывания виртуальной сетевой функции. Эта директория отсутствует в пакете PNF.
- /scripts – скрипты для развертывания и управления сетевой функцией.
- logo.png – значок сетевой функции. Необязательный компонент.
- description-file.pdf – техническая документация или спецификация сетевой функции. Необязательный компонент.

Вам нужно загрузить пакет VNF или PNF в веб-интерфейс оркестратора, чтобы развернуть виртуальную сетевую функцию или физическую сетевую функцию.

Настройка VNF-дескриптора

Вам нужно указать параметры виртуальной сетевой функции в VNF-дескрипторе в формате YAML или XML, после чего добавить VNF-дескриптор в корневую директорию пакета VNF. VNF-дескриптор имеет следующую структуру:

Блок/параметр	Описание
`name`	Имя виртуальной сетевой функции.
`description`	Краткое описание виртуальной сетевой функции.
`description_file`	Имя файла в формате PDF с технической документацией или спецификацией виртуальной сетевой функции. Вам нужно поместить файл в корневую директорию пакета VNF. Пользователи могут посмотреть и скачать файл в веб-интерфейсе оркестратора. Необязательный параметр.
`provider`	Поставщик виртуальной сетевой функции.
`version`	Версия виртуальной сетевой функции.
`external_connections`	Внешние точки подключения виртуальной сетевой функции. Вы можете настроить указанные внешние точки подключения виртуальной сетевой функции в веб-интерфейсе оркестратора.
`internal_connections`	Внутренние точки подключения VDU, входящих в состав виртуальной сетевой функции. Необязательный блок.
`virtual_links`	Виртуальные соединения для связи внутренних точек подключения. Этот блок необходимо указать, если вы указали блок `internal_connections`.
`images`	Образы дисков VDU. Вы можете развернуть несколько VDU с помощью одного образа диска VDU.
`configurations`	Скрипты для выполнения действий на различных стадиях работы виртуальной сетевой функции, например при развертывании виртуальной сетевой функции.
`flavours`	Варианты развертывания виртуальной сетевой функции. Вы можете выбрать один из указанных вариантов развертывания виртуальной сетевой функции в веб-интерфейсе оркестратора.

Блок/параметр	Описание
`scaling`	Параметры масштабирования виртуальной сетевой функции. Необязательный блок.
`user_configurations`	Элементы веб-интерфейса оркестратора, которые добавляются в область настройки виртуальной сетевой функции. Необязательный блок.
`backups`	Задания резервного копирования виртуальной сетевой функции. Необязательный блок.

Пример VNF-дескриптора

```
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

Блок external_connections имеет следующую структуру:

Блок/параметр		Описание
- name		Имя внешней точки подключения.
	description	Краткое описание внешней точки подключения.
	ip	IP-адрес внешней точки подключения. Вам нужно ввести значение в формате XXX.XXX.XXX.XXX, например: 192.168.110.126
	mask	Маска подсети внешней точки подключения. Возможные значения: • Значение в формате XXX.XXX.XXX.XXX, например: 255.255.255.0 Маска подсети назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае маску подсети невозможно изменить. • AUTO – автоматически назначить маску подсети с помощью внешнего DHCP-сервера или скрипта из блока configurations. • MANUAL – маску подсети требуется указать вручную в веб-интерфейсе оркестратора при настройке внешних точек подключения виртуальной сетевой функции.
	gw	IP-адрес шлюза внешней точки подключения. Возможные значения: • Значение в формате XXX.XXX.XXX.XXX, например: 192.168.110.126 IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • AUTO – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока configurations. • MANUAL – IP-адрес требуется указать вручную в веб-интерфейсе оркестратора при настройке внешних точек подключения виртуальной сетевой функции. Необязательный параметр.
	dns	IP-адрес DNS-сервера внешней точки подключения. Возможные значения: • Значение в формате XXX.XXX.XXX.XXX, например: 192.168.110.126 IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • AUTO – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока configurations. • MANUAL – IP-адрес требуется указать вручную в веб-интерфейсе оркестратора при настройке внешних точек подключения виртуальной сетевой функции. Необязательный параметр.
	group	Группа, к которой относится внешняя точка подключения. Этот параметр необходимо указать, если несколько VDU в составе виртуальной сетевой функции используют одну внешнюю точку подключения.

Пример блока

```
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

Блок `internal_connections` имеет следующую структуру:

Блок/параметр		Описание
`- name`		Имя внутренней точки подключения.
	`description`	Краткое описание внутренней точки подключения.
	`virtual_link_name`	Имя виртуального соединения из блока `virtual_links` для внутренней точки подключения.
	`ip`	IP-адрес внутренней точки подключения. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • `AUTO` – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока `configurations`. • `MANUAL` – IP-адрес требуется указать вручную в веб-интерфейсе оркестратора при настройке внешних точек подключения виртуальной сетевой функции.
	`mask`	Маска подсети внутренней точки подключения. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `255.255.255.0` Маска подсети назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае маску подсети невозможно изменить. • `AUTO` – автоматически назначить маску подсети с помощью внешнего DHCP-сервера или скрипта из блока `configurations`.
	`gw`	IP-адрес шлюза внутренней точки подключения. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • `AUTO` – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока `configurations`. Необязательный параметр.
	`dns`	IP-адрес DNS-сервера внутренней точки подключения. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • `AUTO` – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока `configurations`. Необязательный параметр.
	`group`	Группа, к которой относится внутренняя точка подключения. Этот параметр необходимо указать, если несколько VDU в составе виртуальной сетевой функции используют одну внутреннюю точку подключения.

Пример блока

```
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

Блок `virtual_links` имеет следующую структуру:

Блок/параметр		Описание
`- name`		Имя виртуального соединения.
	`cidr`	IPv4-префикс виртуального соединения. Вам нужно ввести значение в формате XXX.XXX.XXX.XXX/XX, например: `192.168.2.0/24`
	`ip_version`	Версия IP-адресов в подсети. Возможные значения: • `v4`; • `v6`.

Пример блока

```
virtual_links:
- name: int_link
  cidr: 203.0.113.0/24
  ip_version: v4
```

images

Блок `images` имеет следующую структуру:

Блок/параметр		Описание
`- name`		Имя образа диска VDU.
	`container_format`	Формат контейнера для образа диска VDU.
	`disk_format`	Формат образа диска VDU.
	`type`	Тип VIM.
	`file_name`	Имя файла образа диска VDU. Вам нужно поместить образ диска VDU в директорию /image пакета VNF.

Пример блока

```
images:
- name: VDU_img
  container_format: BARE
  disk_format: QCOW2
  type: OPENSTACK
  filename: VDU_img.qcow2
```

configurations

Блок `configurations` имеет следующую структуру:

Блок/параметр		Описание
`- name`		Имя скрипта.
	`filename`	Имя файла скрипта, сценария Ansible или атрибута user-data для Cloud-init. Вам нужно поместить скрипт в директорию /scripts пакета VNF.
	`stage`	Стадия работы виртуальной сетевой функции, на которой скрипт запускается. Возможные значения: • `initialization` – запустить скрипт при развертывании виртуальной сетевой функции. • `termination` – запустить скрипт при удалении виртуальной сетевой функции. • `none` – запустить скрипт при изменении значения элемента веб-интерфейса оркестратора из блока `user_configurations` в области настройки виртуальной сетевой функции.
	`executor`	Интерпретатор скрипта. Возможные значения: • `ansible`; • `expect`; • `/bin/sh`; • `bin/bash`; • `cloud-init`; • `< путь к пользовательскому интерпретатору скрипта >`, например `/usr/bin/php`.
	`authentication`	Метод аутентификации VNFM в виртуальной сетевой функции для запуска скриптов. Возможные значения: • `key` – аутентифицировать VNFM в виртуальной сетевой функции по ключу, который генерируется при развертывании виртуальной сетевой функции. Вам нужно получить ключ с помощью скрипта, поэтому мы рекомендуем не указывать это значение для первого скрипта. • `password` – аутентифицировать VNFM в виртуальной сетевой функции по имени и паролю учетной записи из блока `flavours` → `vdus`.
	`files_path`	Путь к файлам для запуска скриптов с помощью SSH. Вам нужно создать директорию в директории /scripts пакета VNF и поместить в созданную директорию файлы. Файлы будут скопированы на VDU. Необязательный параметр.
	`config_drive`	Использование config-drive. Возможные значения: • `true`; • `false`. Этот параметр можно указать, если для параметра `executor` вы указали значение `cloud_init`.
	`timeout`	Время ожидания выполнения скрипта в секундах. Если скрипт не выполняется по истечении указанного времени, выполнение прерывается. Отсчет времени начинается в момент запуска скрипта. Этот параметр можно указать, если для параметра `executor` вы указали путь к пользовательскому исполнителю скрипта.

Пример блока

```
configurations:
  - name: config
    filename: config.yml
    stage: initialization
    executor: ansible
    authentication: password
    files_path: SSH_scripts
    config_drive: true
    timeout: 15
```

flavours

Блок `flavours` имеет следующую структуру:

Блок/параметр		Описание
`- name`		Имя варианта развертывания.
	`description`	Краткое описание варианта развертывания.
	`position`	Порядковый номер варианта развертывания. Вариант развертывания с наименьшим порядковым номером имеет наименьшую производительность.
	`affinity`	Группы VDU, которые размещаются на одном хосте OpenStack. Мы рекомендуем разместить на одном хосте OpenStack VDU, требующие минимальных задержек при обмене информацией друг с другом.
	`anti-affinity`	Группы VDU, которые размещаются на разных хостах OpenStack. Мы рекомендуем развернуть на разных хостах OpenStack VDU, для которых может потребоваться вертикальное масштабирование или обеспечение отказоустойчивости.
	`management`	Параметры консолей администрирования VDU.
	`vdus`	Параметры VDU.

Блоки `affinity` и `anti-affinity` имеют следующую структуру:

Блок/параметр			Описание
`groups`			Группы VDU.
	`- name`		Имя группы VDU.

		`vdu_name`	Имена VDU. Вам нужно указать список значений, например:
			`vdu_name:`
			`- VDU_1`
			`- VDU_2`

Блок `management` имеет следующую структуру:

Блок/параметр		Описание
`vnc`		Параметры управления VDU с помощью VNC-консоли.
	`- vdu_name`	Имя VDU.
`ssh`		Параметры управления VDU с помощью SSH-консоли.

Блок/параметр			Описание
	- vdu_name		Имя VDU.
		def_user	Имя учетной записи для установки SSH-сессии.
		authentication	Метод аутентификации VNFM в виртуальной сетевой функции для запуска скриптов. Возможные значения: • key – аутентифицировать VNFM в виртуальной сетевой функции по ключу, который генерируется при развертывании виртуальной сетевой функции. Вам нужно получить ключ с помощью скрипта из блока configurations. • password – аутентифицировать VNFM в виртуальной сетевой функции по имени и паролю учетной записи из блока vdus.
web			Параметры управления VDU с помощью веб-консоли.
	- vdu_name		Имя VDU.
		protocol	Протокол подключения к веб-консоли. Возможные значения: • http; • https.
		port	Порт подключения к веб-консоли. Вам нужно ввести значение в диапазоне от 1 до 65 536. По умолчанию используется порт 80.
		path	Путь к веб-консоли.
		def_user	Имя учетной записи для аутентификации в веб-консоли.
		def_password	Пароль учетной записи для аутентификации в веб-консоли.

Блок vdus имеет следующую структуру:

Блок/параметр			Описание
`- name`			Имя VDU.
	`password_rules`		Требования к паролю VDU. Необязательный блок.
		`length`	Минимальная длина пароля.
		`use_upper_case`	Пользователи должны использовать прописные символы в пароле. Возможные значения: • `true`; • `false`.
		`use_lower_case`	Пользователи должны использовать строчные символы в пароле. Возможные значения: • `true`; • `false`.
		`use_digits`	Пользователи должны использовать цифры в пароле. Возможные значения: • `true`; • `false`.
		`specific_symbols`	Специальные символы, которые пользователи должны использовать в пароле, например: `@"!`
		`specific_symbols_min_usage`	Минимальное количество специальных символов в пароле.
	`check_connection_mode`		Тип проверки доступности VDU при развертывании. По умолчанию используется SSH-проверка. Возможные значения: • `ssh`; • `none`. Необязательный параметр.
	`zabbix_template`		Имя шаблона Zabbix для VDU.
	`monitoring_type`		Тип мониторинга виртуальной сетевой функции. Возможные значения: • `agent` – мониторинг с помощью Zabbix-агента. • `snmp` – мониторинг с помощью протокола SNMP.
	`ssh_port`		Номер порта для установки SSH-сессии. Необязательный параметр.
	`ssh_host_key_algorithm`		Используемый алгоритм ключа хоста (англ. host key algorithm). Возможные значения: • `ssh-rsa`. • `ssh-ed25519`. Мы рекомендуем использовать этот алгоритм хоста ключа, так как он является криптостойким. Если вы не указываете этот параметр, по умолчанию используется алгоритм ssh-rsa для обеспечения обратной совместимости.

	`configurations`		Имена скриптов из блока `configurations`, которые запускаются на VDU. Вам нужно указать список значений, например:
			`vdu_name:`
			`- config_1`
			`- config_2`

	`backups`		Имена заданий резервного копирования из блока `backups`, которые используются на VDU. Вам нужно указать список значений, например:
			`vdu_name:`
			`- backup_1`
			`- backup_2`
			Необязательный блок.

Блок/параметр	Описание
`def_user`	Имя учетной записи для аутентификации VNFM в виртуальной сетевой функции. Необязательный параметр.
`def_password`	Пароль учетной записи для аутентификации VNFM в виртуальной сетевой функции. Необязательный параметр.
`password_authentication`	Аутентификация VNFM в виртуальной сетевой функции по паролю. Возможные значения: • `yes`; • `no`. Необязательный параметр.
`disks`	Параметры виртуальных дисков VDU.
`- name`	Имя виртуального диска VDU.
`order`	Порядок подключения виртуального диска VDU.
`type`	Тип эфемерного диска OpenStack.
`image`	Имя образа виртуального диска VDU из блока `images`. Необязательный параметр, если вы создаете пустой диск VDU.
`storage_db`	Размер виртуального диска VDU в гигабайтах.
`cpu`	Параметры процессора VDU.
`smt`	Требования к одновременной гиперпоточности (англ. simultaneous multithreading) при развертывании VDU. Возможные значения: • `prefer` – использовать одновременную гиперпоточность, если она включена на хосте VDU. • `isolate` – не использовать одновременную гиперпоточность. • `require` – использовать одновременную гиперпоточность.
`cpu_pinning`	Использование привязки процессора (англ. CPU pinning). Возможные значения: • `shared` – не привязывать ядра процессора к VDU. • `dedicated` – привязывать ядра процессора к VDU.
`num_vpu`	Количество привязываемых к VDU ядер процессора.
`memory`	Параметры оперативной памяти VDU.
`total_memory_mb`	Количество оперативной памяти VDU в мегабайтах.
`page_size`	Размер страниц памяти при развертывании VDU. Возможные значения: • `small` – 4 КБ. • `large` – 2 МБ или 1 ГБ. • `any` – любой размер. • `4KB`. • `2MB`. • `2048`. • `1GB`.
`network_interfaces`	Параметры сетевых интерфейсов.

Блок/параметр	Описание
- name	Имя сетевого интерфейса.
type	Тип сетевого интерфейса. Возможные значения: • `data` – сетевой интерфейс для передачи данных. • `management` – управляющий сетевой интерфейс, который ссылается на сетевой порт.
description	Краткое описание сетевого интерфейса.
connection_point_ref	Имя внешней точки подключения из блока `external_connections` для управляющего сетевого интерфейса.
port_security	Использование функции Port security. Возможные значения: • `disabled`; • `enabled`. Необязательный параметр.
properties	Дополнительные параметры сетевого интерфейса.
vnic_type	vNIC-тип сетевого интерфейса. Возможные значения: • `virtio`; • `direct`; • `macvtap`; • `vhost`.
auto_healing	Параметры автоматического восстановления VDU.
triggers_set	Внешние триггеры, при срабатывании которых начинается автоматическое восстановление VDU. Возможные значения: • `any` – автоматическое восстановление VDU начинается, если срабатывает любой из указанных внешних триггеров. • `all` – автоматическое восстановление VDU начинается, если срабатывают все указанные внешние триггеры. • `< имя триггера >` – автоматическое восстановление VDU начинается, если срабатывает указанный внешний триггер.
triggers	Внешние триггеры.
- name	Имя внешнего триггера. Возможные значения: • `unreachable`; • `scale_up`; • `scale_down`.
action_set	Действие, которое выполняется при срабатывании внешнего триггера.
- type	Тип действия. Возможные значения: • `reprovision` – повторно развернуть VDU; • `reboot` – перезагрузить VDU; • `script` – запустить указанный скрипт.
configuration_name_ref	Имя скрипта из блока `configurations`, который запускается при срабатывании внешнего триггера. Этот параметр необходимо указать, если для параметра `- type` вы указали значение `script`.
bootstrap_timeout	Время ожидания доступности по SSH при развертывании VDU в секундах. Если VDU не доступна по SSH по истечении указанного времени, происходит откат развертывания. Необязательный параметр.

[Пример блока]

```
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

Блок `scaling` имеет следующую структуру:

Параметр	Описание
`scale_in_status`	Горизонтальное масштабирование до варианта развертывания с более низким порядковым номером. Возможные значения: • `permit`; • `deny`.
`scale_out_status`	Горизонтальное масштабирование до варианта развертывания с более высоким порядковым номером. Возможные значения: • `permit`; • `deny`.
`scale_up_status`	Вертикальное масштабирование до варианта развертывания с более низким порядковым номером. Возможные значения: • `permit`; • `deny`.
`scale_down_status`	Вертикальное масштабирование до варианта развертывания с более высоким порядковым номером. Возможные значения: • `permit`; • `deny`.

Пример блока

```
scaling:
  scale_in_status: permit
  scale_out_status: permit
  scale_up_status: permit
  scale_down_status: permit
```

user_configurations

Блок `user_configurations` имеет следующую структуру:

Блок/параметр	Описание
`tab`	Вкладки, которые добавляются в область настройки виртуальной сетевой функции.
`- name`	Имя вкладки.

Блок/параметр			Описание
	`variables`		Элементы веб-интерфейса оркестратора, которые отображаются на вкладке.
	`- name`		Имя элемента веб-интерфейса оркестратора.
		`description`	Краткое описание элемента веб-интерфейса оркестратора.
		`input_type`	Тип элемента веб-интерфейса оркестратора. Возможные значения: • `input` – поле. • `dropdown` – раскрывающийся список.
		`default_value`	Значение по умолчанию в поле. Этот параметр можно указать, если для параметра `input_type` вы указали значение `input`.
		`values`	Значения, которые отображаются в раскрывающемся списке. Этот блок можно указать, если для параметра `input_type` вы указали значение `dropdown`.
		`- value`	Имя значения.
		`is_default`	Значение по умолчанию. Возможные значения: • `true`; • `false`. Необязательный параметр.
		`required`	Обязательный элемент веб-интерфейса оркестратора. Возможные значения: • `true`; • `false`. Необязательный параметр.
		`type`	Тип значения, которое может быть указано для элемента веб-интерфейса оркестратора. Необязательный параметр.
		`example`	Подсказка, которая отображается при изменении значения элемента веб-интерфейса оркестратора. Необязательный параметр.

		`update_configuration_name`	Имена скриптов из блока `configurations`, которые запускаются при изменении значения элемента веб-интерфейса оркестратора. Вам нужно указать список значений, например:
			`update_configuration_name:`
			`- config_1`
			`- config_2`

[Пример блока](#)

```
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

Блок backups имеет следующую структуру:

Блок/параметр			Описание
`- name`			Имя задания резервного копирования.
	`description`		Краткое описание задания резервного копирования.
	`backup`		Параметры резервного копирования.
		`path`	Путь к директории виртуальной сетевой функции, в которой содержатся файлы для резервного копирования.
		`interval`	Интервал времени в секундах для резервного копирования.
		`store_config`	Количество хранимых резервных копий.
		`backup_type`	Тип резервного копирования.
		`authentication`	Метод аутентификации VNFM в виртуальной сетевой функции для запуска скриптов. Возможные значения: • `key` – аутентифицировать VNFM в виртуальной сетевой функции по ключу, который генерируется при развертывании виртуальной сетевой функции. Вам нужно получить ключ с помощью скрипта из блока `configurations`. • `password` – аутентифицировать VNFM в виртуальной сетевой функции по имени и паролю учетной записи из блока `flavours` → `vdus`.
		`configuration_name_ref`	Имя скрипта из блока `configurations`, который запускается перед резервным копированием.
	`restore`		Параметры восстановления из резервной копии.
		`path`	Путь к директории виртуальной сетевой функции, в которую помещаются восстановленные файлы.
		`backup_type`	Тип резервного копирования.
		`authentication`	Метод аутентификации VNFM в виртуальной сетевой функции для запуска скриптов. Возможные значения: • `key` – аутентифицировать VNFM в виртуальной сетевой функции по ключу, который генерируется при развертывании виртуальной сетевой функции. Вам нужно получить ключ с помощью скрипта из блока `configurations`. • `password` – аутентифицировать VNFM в виртуальной сетевой функции по имени и паролю учетной записи из блока `flavours` → `vdus`.
		`configuration_name_ref`	Имя скрипта из блока `configurations`, который запускается после восстановления резервной копии.

Пример блока

```
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
```

Настройка PNF-дескриптора

Вам нужно указать параметры физической сетевой функции в PNF-дескрипторе в формате YAML или XML, после чего добавить PNF-дескриптор в корневую директорию пакета PNF. PNF-дескриптор имеет следующую структуру:

Блок/параметр	Описание
`name`	Имя физической сетевой функции.
`description`	Краткое описание физической сетевой функции.
`description_file`	Имя файла в формате PDF с технической документацией или спецификацией физической сетевой функции. Вам нужно поместить файл в корневую директорию пакета PNF. Пользователи могут посмотреть и скачать файл в веб-интерфейсе оркестратора. Необязательный параметр.
`provider`	Поставщик физической сетевой функции.
`version`	Версия физической сетевой функции.
`external_connections`	Внешние точки подключения физической сетевой функции.
`internal_connections`	Внутренние точки подключения VDU, входящих в состав физической сетевой функции. Необязательный блок.
`configurations`	Скрипты для выполнения действий на различных стадиях работы физической сетевой функции, например при развертывании физической сетевой функции.
`flavours`	Варианты развертывания физической сетевой функции. Вы можете выбрать один из указанных вариантов развертывания физической сетевой функции в веб-интерфейсе оркестратора.
`scaling`	Параметры масштабирования физической сетевой функции. Необязательный блок.
`user_configurations`	Элементы веб-интерфейса оркестратора, которые добавляются в область настройки физической сетевой функции. Необязательный блок.
`backups`	Задания резервного копирования физической сетевой функции. Необязательный блок.

Пример PNF-дескриптора

```
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

Блок external_connections имеет следующую структуру:

Блок/параметр		Описание
`- name`		Имя внешней точки подключения.
	`description`	Краткое описание внешней точки подключения.
	`ip`	IP-адрес внешней точки подключения. Вам нужно ввести значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126`
	`mask`	Маска подсети внешней точки подключения. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `255.255.255.0` Маска подсети назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае маску подсети невозможно изменить. • `AUTO` – автоматически назначить маску подсети с помощью внешнего DHCP-сервера или скрипта из блока `configurations`.
	`gw`	IP-адрес шлюза внешней точки подключения. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • `AUTO` – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока `configurations`. Необязательный параметр.
	`dns`	IP-адрес DNS-сервера внешней точки подключения. Возможные значения: • Значение в формате `XXX.XXX.XXX.XXX`, например: `192.168.110.126` IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • `AUTO` – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока `configurations`. Необязательный параметр.
	`group`	Группа, к которой относится внешняя точка подключения. Этот параметр необходимо указать, если несколько VDU в составе физической сетевой функции используют одну внешнюю точку подключения.

Пример блока

```
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`

Блок `internal_connections` имеет следующую структуру:

Блок/параметр		Описание
- name		Имя внутренней точки подключения.
	description	Краткое описание внутренней точки подключения.
	ip	IP-адрес внутренней точки подключения. Возможные значения: • Значение в формате XXX.XXX.XXX.XXX, например: 192.168.110.126 IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • AUTO – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока configurations.
	mask	Маска подсети внутренней точки подключения. Возможные значения: • Значение в формате XXX.XXX.XXX.XXX, например: 255.255.255.0 Маска подсети назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае маску подсети невозможно изменить. • AUTO – автоматически назначить маску подсети с помощью внешнего DHCP-сервера или скрипта из блока configurations.
	gw	IP-адрес шлюза внутренней точки подключения. Возможные значения: • Значение в формате XXX.XXX.XXX.XXX, например: 192.168.110.126 IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • AUTO – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока configurations. Необязательный параметр.
	dns	IP-адрес DNS-сервера внутренней точки подключения. Возможные значения: • Значение в формате XXX.XXX.XXX.XXX, например: 192.168.110.126 IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта. В этом случае IP-адрес невозможно изменить. • AUTO – автоматически назначить IP-адрес с помощью внешнего DHCP-сервера или скрипта из блока configurations. Необязательный параметр.
	group	Группа, к которой относится внутренняя точка подключения. Этот параметр необходимо указать, если несколько VDU в составе физической сетевой функции используют одну внутреннюю точку подключения.

Пример блока

```
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

Блок configurations имеет следующую структуру:

Блок/параметр		Описание
`- name`		Имя скрипта.
	`filename`	Имя файла скрипта или сценария Ansible. Вам нужно поместить скрипт в директорию /scripts пакета PNF.
	`stage`	Стадия работы физической сетевой функции, на которой скрипт запускается. Возможные значения: • `initialization` – запустить скрипт при развертывании физической сетевой функции. • `termination` – запустить скрипт при удалении физической сетевой функции. • `none` – запустить скрипт при изменении значения элемента веб-интерфейса оркестратора из блока `user_configurations` в области настройки физической сетевой функции.
	`executor`	Интерпретатор скрипта. Возможные значения: • `ansible`; • `expect`; • `/bin/sh`; • `bin/bash`; • `< путь к пользовательскому интерпретатору скрипта >`, например `/usr/bin/php`.
	`authentication`	Метод аутентификации VNFM в физической сетевой функции для запуска скриптов. Возможные значения: • `key` – аутентифицировать VNFM в физической сетевой функции по ключу, который генерируется при развертывании физической сетевой функции. Вам нужно получить ключ с помощью скрипта, поэтому мы рекомендуем не указывать это значение для первого скрипта. • `password` – аутентифицировать VNFM в физической сетевой функции по имени и паролю учетной записи из блока `flavours` → `vdus`.
	`files_path`	Путь к файлам для запуска скриптов с помощью SSH. Вам нужно создать директорию в директории /scripts пакета PNF и поместить в созданную директорию файлы. Файлы будут скопированы на VDU. Необязательный параметр.
	`timeout`	Время ожидания выполнения скрипта в секундах. Если скрипт не выполняется по истечении указанного времени, выполнение прерывается. Отсчет времени начинается в момент запуска скрипта. Этот параметр можно указать, если для параметра `executor` вы указали путь к пользовательскому исполнителю скрипта.

Пример блока

```
configurations:
  - name: config
    filename: config.yml
    stage: initialization
    executor: ansible
    authentication: password
    files_path: SSH_scripts
    config_drive: true
    timeout: 15
```

`flavours`

Блок `flavours` имеет следующую структуру:

Блок/параметр		Описание
- name		Имя варианта развертывания.
	description	Краткое описание варианта развертывания.
	position	Порядковый номер варианта развертывания. Вариант развертывания с наименьшим порядковым номером имеет наименьшую производительность.
	management	Параметры консолей администрирования VDU.
	vdus	Параметры VDU.

Блок management имеет следующую структуру:

Блок/параметр			Описание
ssh			Параметры управления VDU с помощью SSH-консоли.
	- vdu_name		Имя VDU.
		def_user	Имя учетной записи для установки SSH-сессии.
		authentication	Метод аутентификации VNFM в физической сетевой функции для запуска скриптов. Возможные значения: • key – аутентифицировать VNFM в физической сетевой функции по ключу, который генерируется при развертывании физической сетевой функции. Вам нужно получить ключ с помощью скрипта из блока configurations. • password – аутентифицировать VNFM в физической сетевой функции по имени и паролю учетной записи из блока vdus.
web			Параметры управления VDU с помощью веб-консоли.
	- vdu_name		Имя VDU.
		protocol	Протокол подключения к веб-консоли. Возможные значения: • http; • https.
		port	Порт подключения к веб-консоли. Вам нужно ввести значение в диапазоне от 1 до 65 536. По умолчанию используется порт 80.
		path	Путь к веб-консоли.
		def_user	Имя учетной записи для аутентификации в веб-консоли.
		def_password	Пароль учетной записи для аутентификации в веб-консоли.

Блок vdus имеет следующую структуру:

Блок/параметр	Описание
`- name`	Имя VDU.
`password_rules`	Требования к паролю VDU. Необязательный блок.
`length`	Минимальная длина пароля.
`use_upper_case`	Пользователи должны использовать прописные символы в пароле. Возможные значения: • `true`; • `false`.
`use_lower_case`	Пользователи должны использовать строчные символы в пароле. Возможные значения: • `true`; • `false`.
`use_digits`	Пользователи должны использовать цифры в пароле. Возможные значения: • `true`; • `false`.
`specific_symbols`	Специальные символы, которые пользователи должны использовать в пароле, например: `@"!`
`specific_symbols_min_usage`	Минимальное количество специальных символов в пароле.
`check_connection_mode`	Тип проверки доступности VDU при развертывании. По умолчанию используется SSH-проверка. Возможные значения: • `ssh`; • `none`. Необязательный параметр.
`zabbix_template`	Имя шаблона Zabbix для VDU.
`monitoring_type`	Тип мониторинга физической сетевой функции. Возможные значения: • `agent` – мониторинг с помощью Zabbix-агента. • `snmp` – мониторинг с помощью протокола SNMP.
`ssh_port`	Номер порта для установки SSH-сессии. Необязательный параметр.
`ssh_host_key_algorithm`	Используемый алгоритм ключа хоста (англ. host key algorithm). Возможные значения: • `ssh-rsa`. • `ssh-ed25519`. Мы рекомендуем использовать этот алгоритм хоста ключа, так как он является криптостойким. Если вы не указываете этот параметр, по умолчанию используется алгоритм ssh-rsa для обеспечения обратной совместимости.

`configurations`	Имена скриптов из блока `configurations`, которые запускаются на VDU. Вам нужно указать список значений, например:
	`vdu_name:`
	`- config_1`
	`- config_2`

`backups`	Имена заданий резервного копирования из блока `backups`, которые используются на VDU. Вам нужно указать список значений, например:
	`vdu_name:`
	`- backup_1`
	`- backup_2`
	Необязательный блок.

Блок/параметр	Описание
def_user	Имя учетной записи для аутентификации VNFM в физической сетевой функции. Необязательный параметр.
def_password	Пароль учетной записи для аутентификации VNFM в физической сетевой функции. Необязательный параметр.
password_authentication	Аутентификация VNFM в физической сетевой функции по паролю. Возможные значения: • yes; • no. Необязательный параметр.
network_interfaces	Параметры сетевых интерфейсов.
- name	Имя сетевого интерфейса.
type	Тип сетевого интерфейса. Возможные значения: • data – сетевой интерфейс для передачи данных. • management – управляющий сетевой интерфейс, который ссылается на сетевой порт.
description	Краткое описание сетевого интерфейса.
connection_point_ref	Имя внешней точки подключения из блока external_configurations для управляющего сетевого интерфейса.
auto_healing	Параметры автоматического восстановления VDU.
triggers_set	Внешние триггеры, при срабатывании которых начинается автоматическое восстановление VDU. Возможные значения: • any – автоматическое восстановление VDU начинается, если срабатывает любой из указанных внешних триггеров. • all – автоматическое восстановление VDU начинается, если срабатывают все указанные внешние триггеры. • < имя триггера > – автоматическое восстановление VDU начинается, если срабатывает указанный внешний триггер.
triggers	Внешние триггеры.
- name	Имя внешнего триггера. Возможные значения: • unreachable; • scale_up; • scale_down.
action_set	Действие, которое выполняется при срабатывании внешнего триггера.
- type	Тип действия. Возможные значения: • reboot – перезагрузить VDU; • script – запустить указанный скрипт.
configuration_name_ref	Имя скрипта из блока configurations, который запускается при срабатывании внешнего триггера. Этот параметр необходимо указать, если для параметра - type вы указали значение script.

[Пример блока]

```
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

Блок `scaling` имеет следующую структуру:

Параметр	Описание
`scale_up_status`	Вертикальное масштабирование до варианта развертывания с более низким порядковым номером. Возможные значения: • `permit`; • `deny`.
`scale_down_status`	Вертикальное масштабирование до варианта развертывания с более высоким порядковым номером. Возможные значения: • `permit`; • `deny`.

Пример блока

```
scaling:
  scale_in_status: permit
  scale_out_status: permit
```

user_configurations

Блок `user_configurations` имеет следующую структуру:

Блок/параметр	Описание
`tab`	Вкладки, которые добавляются в область настройки физической сетевой функции.
`- name`	Имя вкладки.
`variables`	Элементы веб-интерфейса оркестратора, которые отображаются на вкладке.
`- name`	Имя элемента веб-интерфейса оркестратора.
`description`	Краткое описание элемента веб-интерфейса оркестратора.
`input_type`	Тип элемента веб-интерфейса оркестратора. Возможные значения: • `input` – поле. • `dropdown` – раскрывающийся список.
`default_value`	Значение по умолчанию в поле. Этот параметр можно указать, если для параметра `input_type` вы указали значение `input`.
`values`	Значения, которые отображаются в раскрывающемся списке. Этот блок можно указать, если для параметра `input_type` вы указали значение `dropdown`.
`- value`	Имя значения.
`is_default`	Значение по умолчанию. Возможные значения: • `true`; • `false`. Необязательный параметр.
`required`	Обязательный элемент веб-интерфейса оркестратора. Возможные значения: • `true`; • `false`. Необязательный параметр.
`type`	Тип значения, которое может быть указано для элемента веб-интерфейса оркестратора. Необязательный параметр.
`example`	Подсказка, которая отображается при изменении значения элемента веб-интерфейса оркестратора. Необязательный параметр.

`update_configuration_name`	Имена скриптов из блока `configurations`, которые запускаются при изменении значения элемента веб-интерфейса оркестратора. Вам нужно указать список значений, например:
	`update_configuration_name:`
	`- config_1`
	`- config_2`

Пример блока

```
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

Блок backups имеет следующую структуру:

Блок/параметр			Описание
`- name`			Имя задания резервного копирования.
	`description`		Краткое описание задания резервного копирования.
	`backup`		Параметры резервного копирования.
		`path`	Путь к директории физической сетевой функции, в которой содержатся файлы для резервного копирования.
		`interval`	Интервал времени в секундах для резервного копирования.
		`store_config`	Количество хранимых резервных копий.
		`backup_type`	Тип резервного копирования.
		`authentication`	Метод аутентификации VNFM в физической сетевой функции для запуска скриптов. Возможные значения: • `key` – аутентифицировать VNFM в физической сетевой функции по ключу, который генерируется при развертывании физической сетевой функции. Вам нужно получить ключ с помощью скрипта из блока `configurations`. • `password` – аутентифицировать VNFM в физической сетевой функции по имени и паролю учетной записи из блока `flavours` → `vdus`.
		`configuration_name_ref`	Имя скрипта из блока `configurations`, который запускается перед резервным копированием.
	`restore`		Параметры восстановления из резервной копии.
		`path`	Путь к директории физической сетевой функции, в которую помещаются восстановленные файлы.
		`backup_type`	Тип резервного копирования.
		`authentication`	Метод аутентификации VNFM в физической сетевой функции для запуска скриптов. Возможные значения: • `key` – аутентифицировать VNFM в физической сетевой функции по ключу, который генерируется при развертывании физической сетевой функции. Вам нужно получить ключ с помощью скрипта из блока `configurations`. • `password` – аутентифицировать VNFM в физической сетевой функции по имени и паролю учетной записи из блока `flavours` → `vdus`.
		`configuration_name_ref`	Имя скрипта из блока `configurations`, который запускается после восстановления резервной копии.

Пример блока

```
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
```

Защита пакетов VNF и PNF от подмены и изменения

Часть файлов пакетов VNF и PNF помещается в локальную директорию Docker-контейнера оркестратора, и вы можете защитить их от подмены и изменения. Когда пакеты VNF и PNF защищены, оркестратор автоматически считает их хеш-сумму SHA256 при загрузке в веб-интерфейс оркестратора. При обращении к файлам в локальной директории Docker-контейнера оркестратор сравнивает их текущую хеш-сумму SHA256 с ранее сохраненной. Если хеш-суммы SHA256 не совпадают, оркестратор лишает пользователей возможности выполнять действия с сетевой функцией, например добавлять ее в топологию сетевого сервиса.

Чтобы защитить пакеты VNF и PNF от подмены и изменения:

1. В меню перейдите в раздел **Система**.

   По умолчанию выбрана вкладка **Мониторинг**, на которой отображаются параметры подключения к серверу Zabbix.

2. Выберите вкладку **Другое** и установите флажок **Вычислять хеш-сумму SHA256 для файлов VNF/PNF в хранилище**. Этот флажок установлен по умолчанию.

Пакеты VNF и PNF будут защищены от подмены и изменения.

Загрузка пакета VNF или PNF в веб-интерфейс оркестратора

Чтобы загрузить пакет VNF или PNF в веб-интерфейс оркестратора:

1. В меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В верхней части страницы нажмите на кнопку **+ VNF** или **+ PNF**.

3. В открывшемся окне выберите пакет VNF или PNF.

4. Если вы хотите проверить целостность пакета VNF или PNF, в поле **Хеш-сумма SHA256** введите его хеш-сумму SHA256. Максимальная длина хеш-суммы: 64 символа.

5. Нажмите на кнопку **Сохранить**.

Пакет VNF или PNF будет загружен в веб-интерфейс оркестратора. VNF или PNF отобразится в панели **Каталог**. Если вы ввели хеш-сумму SHA256 пакета VNF или PNF, оркестратор сравнит введенное значение с реальной хеш-суммой SHA256. При несовпадении хеш-сумм SHA256 пакет VNF или PNF не будет загружен.

Указание краткого описания общего сетевого сервиса

Чтобы указать краткое описание общего сетевого сервиса:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.

   - Начните создание или изменение сетевого сервиса.

2. В графическом конструкторе нажмите на общий сетевой сервис, краткое описание которого вы хотите указать.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию будет выбрана вкладка **Параметры**, на которой отображается краткое описание общего сетевого сервиса.

3. В поле **Описание** введите краткое описание общего сетевого сервиса.

4. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры общего сетевого сервиса.

Работа с виртуальными сетевыми функциями

Для работы с виртуальной сетевой функцией вам нужно выполнить одно из следующих действий:

- на портале администратора перейти в раздел **Каталог** и в панели **Каталог** нажать на виртуальную сетевую функцию;

- при создании или изменении шаблона сетевого сервиса в топологии нажать на виртуальную сетевую функцию;

- при создании или изменении сетевого сервиса в топологии нажать на виртуальную сетевую функцию.

Параметры виртуальной сетевой функции можно настроить на следующих вкладках:

- **Варианты развертывания** – варианты развертывания виртуальной сетевой функции.

- **Точки подключения** – внешние точки подключения виртуальной сетевой функции.

- **Параметры VNF** – основные параметры виртуальной сетевой функции.

- **Размещение** – параметры размещения виртуальной сетевой функции. Вы можете разместить виртуальную сетевую функцию в центре обработки данных или на устройстве uCPE. Эта вкладка отображается, если вы нажали на виртуальную сетевую функцию при создании или изменении сетевого сервиса.

Следующие вкладки отображаются, если вы нажали на виртуальную сетевую функцию в топологии развернутого сетевого сервиса:

- **Управление VDU** – таблица VDU, входящих в состав виртуальной сетевой функции. Информация о VDU отображается в следующих столбцах таблицы:
  - **Имя** – имя VDU.
  - **Имя экземпляра** – идентификатор экземпляра VDU.
  - **Mgmt IP** – IP-адрес, который подсеть управления назначила VDU.
  - **vCPU** – количество назначенных VDU виртуальных ядер процессора.
  - **ОЗУ** – количество назначенной VDU оперативной памяти в мегабайтах.
  - **Диск** – количество назначенного VDU дискового пространства в гигабайтах.
  - **Статус** – статус VDU:
    - **ACTIVE** – VDU работает нормально.
    - **ERROR** – при работе VDU произошла ошибка.
    - **HARD_REBOOT** – выполняется аппаратная перезагрузка VDU.
    - **PAUSED** – VDU поставлена на паузу.
    - **REBOOT** – выполняется программная перезагрузка VDU.
    - **SHUTOFF** – VDU остановлена.
    - **SUSPENDED** – VDU переведена в состояние сна.
- **Мониторинг** – результаты мониторинга виртуальной сетевой функции.
- **Проблемы** – проблемы, возникшие при работе виртуальной сетевой функции. При наличии проблем рядом со вкладкой отображается красный восклицательный знак.

Дополнительно могут отображаться вкладки, которые вы указали в блоке `user_configurations` VNF-дескриптора.

Выбор варианта развертывания виртуальной сетевой функции

Вы можете указать варианты развертывания в блоке `flavours` VNF-дескриптора.

Чтобы выбрать вариант развертывания виртуальной сетевой функции:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.

   - Начните создание или изменение сетевого сервиса.

2. Нажмите на виртуальную сетевую функцию, вариант развертывания которой вы хотите выбрать.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

3. Выберите вариант развертывания виртуальной сетевой функции.

4. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры виртуальной сетевой функции.

Настройка внешних точек подключения виртуальной сетевой функции

Вы можете указать внешние точки подключения виртуальной сетевой функции в блоке `external_connections` VNF-дескриптора.

Чтобы настроить внешние точки подключения виртуальной сетевой функции:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.

   - Начните создание или изменение сетевого сервиса.

2. Нажмите на виртуальную сетевую функцию, внешние точки подключения которой вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

3. Выберите вкладку **Точки подключения**.

   Отобразятся внешние точки подключения виртуальной сетевой функции.

4. В раскрывающемся списке **Тип** выберите, как вы хотите назначить внешней точке подключения IPv4-префикс:

   - **DHCP reservation** – назначить внешней точке подключения IPv4-префикс с помощью DHCP. При выборе этого значения выполните следующие действия:

     a. В поле **IP** введите IPv4-адрес, который DHCP назначает внешней точке подключения.

     b. В поле **Маска** введите маску подсети, которую DHCP назначает внешней точке подключения.

   - **AUTO** – автоматически назначить внешней точке подключения IPv4-префикс. Это значение выбрано по умолчанию.

5. В поле **Описание** введите краткое описание внешней точки подключения.

6. Если вы хотите назначить точку подключения магистральным портом (англ. trunk port), установите флажок **Магистраль**. Этот флажок снят по умолчанию.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры виртуальной сетевой функции.

Настройка основных параметров виртуальной сетевой функции

Чтобы настроить основные параметры виртуальной сетевой функции:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.

   - Начните создание или изменение сетевого сервиса.

2. Нажмите на виртуальную сетевую функцию, основные параметры которой вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ⤢. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

3. Выберите вкладку **Параметры VNF**.

   Отобразятся основные параметры виртуальной сетевой функции.

4. В поле **Имя** введите имя виртуальной сетевой функции.

5. В поле **Описание** введите краткое описание виртуальной сетевой функции.

6. В поле **Порядок** введите порядковый номер развертывания виртуальной сетевой функции в облачной платформе OpenStack. Когда вы развертываете сетевой сервис, виртуальная сетевая функция с наименьшим значением порядкового номера развертывается первой. Если в параметрах ни одной из добавленных в топологию виртуальных сетевых функций не указан порядковый номер, все виртуальные сетевые функции развертываются одновременно.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры виртуальной сетевой функции.

Размещение виртуальной сетевой функции в центре обработки данных и на устройстве uCPE

Чтобы разместить виртуальную сетевую функцию в центре обработки данных или на устройстве uCPE:

1. Перейдите к топологии, начав создание или изменение сетевого сервиса.

2. Нажмите на виртуальную сетевую функцию, которую вы хотите разместить в центре обработки данных или на устройстве uCPE.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

3. Выберите вкладку **Размещение**.

   Отобразятся параметры размещения виртуальной сетевой функции.

4. В списке **Выберите способ размещения** выберите одно из следующих значений:

   - **Центр обработки данных** – разместить виртуальную сетевую функцию в указанном центре обработки данных. При выборе этого значения выполните следующие действия:

     a. В поле **Центр обработки данных** введите имя созданного центра обработки данных. По мере ввода имени вам предлагается выбрать в раскрывающемся списке центр обработки данных.

     b. В поле **VIM** введите имя развернутого VIM для виртуальной сетевой функции. По мере ввода имени вам предлагается выбрать в раскрывающемся списке VIM.

   - **uCPE** – разместить виртуальную сетевую функцию на указанном устройстве uCPE. При выборе этого значения в поле **uCPE** введите имя устройства uCPE. По мере ввода имени вам предлагается выбрать в раскрывающемся списке устройство uCPE.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры виртуальной сетевой функции.

Остановка и запуск виртуальной сетевой функции или входящей в ее состав VDU

Вы можете остановить виртуальную сетевую функцию или входящую в ее состав VDU, чтобы освободить занимаемые ей вычислительные ресурсы облачной платформы OpenStack.

Когда вы запускаете виртуальную сетевую функцию или VDU, она снова занимает вычислительные ресурсы. При этом процессы, выполняемые на виртуальной сетевой функции или VDU, начинаются заново.

Чтобы остановить или запустить виртуальную сетевую функцию или входящую в ее состав VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Если вы хотите остановить или запустить виртуальную сетевую функцию, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** → **Остановить VNF** или **Запустить VNF**.

5. Если вы хотите остановить или запустить входящую в состав виртуальной сетевой функции VDU, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление** → **Питание** → **Остановить VDU** или **Запустить VDU** рядом с VDU, которую вы хотите остановить или запустить.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Виртуальная сетевая функция или входящая в ее состав VDU будет остановлена или запущена.

Пауза и снятие с паузы виртуальной сетевой функции или входящей в ее состав VDU

Вы можете поставить на паузу виртуальную сетевую функцию или входящую в ее состав VDU, чтобы приостановить выполняемые на ней процессы. При этом виртуальная сетевая функция или VDU продолжает занимать вычислительные ресурсы облачной платформы OpenStack. Когда вы снимаете с паузы виртуальную сетевую функцию или VDU, выполняемые на ней процессы возобновляются.

Чтобы поставить на паузу или снять с паузы виртуальную сетевую функцию или входящую в ее состав VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Поставьте или снимите с паузы виртуальную сетевую функцию или входящую в ее состав VDU:

   - Если вы хотите поставить на паузу или снять с паузы виртуальную сетевую функцию, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** → **Поставить VNF на паузу** или **Снять паузу с VNF**.

   - Если вы хотите поставить на паузу или снять с паузы входящую в состав виртуальной сетевой функции VDU, выполните следующие действия:

     1. Выберите вкладку **Управление VDU**.

        Отобразится таблица VDU.

     2. Нажмите на кнопку **Управление** → **Питание** → **Поставить VDU на паузу** или **Снять паузу с VDU**.

5. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Виртуальная сетевая функция или входящая в ее состав VDU будет поставлена на паузу или снята с паузы.

Перевод виртуальной сетевой функции или входящей в ее состав VDU в состояние сна и активное состояние

Вы можете перевести виртуальную сетевую функцию или входящую в ее состав VDU в состояние сна (англ. suspend), чтобы освободить занимаемые ей вычислительные ресурсы облачной платформы OpenStack. При этом состояние виртуальной сетевой функции или VDU сохраняется на диск облачной платформы OpenStack. Когда вы переводите виртуальную сетевую функцию или VDU в активное состояние (англ. unsuspend), она снова занимает вычислительные ресурсы. Процессы, выполняемые на виртуальной сетевой функции или VDU, возобновляются с момента сохранения ее состояния.

Чтобы перевести виртуальную сетевую функцию или входящую в ее состав VDU в состояние сна или активное состояние:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Переведите виртуальную сетевую функцию или входящую в ее состав VDU в состояние сна или активное состояние:

   - Если вы хотите перевести виртуальную сетевую функцию в состояние сна или активное состояние, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** → **Приостановить VNF** или **Возобновить приостановленную VNF**.

   - Если вы хотите перевести входящую в состав виртуальной сетевой функции VDU в состояние сна или активное состояние, выполните следующие действия:

     1. Выберите вкладку **Управление VDU**.

        Отобразится таблица VDU.

     2. Нажмите на кнопку **Управление** → **Питание** → **Приостановить VDU** или **Возобновить приостановленную VDU** рядом с VDU, которую вы хотите перевести в состояние сна или активное состояние.

5. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Виртуальная сетевая функция или входящая в ее состав VDU будет переведена в состояние сна или активное состояние.

Программная перезагрузка виртуальной сетевой функции или входящей в ее состав VDU

При программной перезагрузке виртуальной сетевой функции перезагружаются все входящие в ее состав активные VDU. Для программной перезагрузки виртуальной сетевой функции хотя бы одна VDU в ее составе должна быть в активном состоянии.

Чтобы выполнить программную перезагрузку виртуальной сетевой функции или входящей в ее состав VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Выполните программную перезагрузку виртуальной сетевой функции или входящей в ее состав VDU:

   - Если вы хотите выполнить программную перезагрузку виртуальной сетевой функции, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** → **Программная перезагрузка VNF**.

   - Если вы хотите выполнить программную перезагрузку входящей в состав виртуальной сетевой функции VDU, выполните следующие действия:

     1. Выберите вкладку **Управление VDU**.

        Отобразится таблица VDU.

     2. Нажмите на кнопку **Управление** → **Питание** → **Программная перезагрузка VDU** рядом с VDU, программную перезагрузку которой вы хотите выполнить.

5. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Будет выполнена программная перезагрузка виртуальной сетевой функции или входящей в ее состав VDU.

Аппаратная перезагрузка виртуальной сетевой функции или входящей в ее состав VDU

При аппаратной перезагрузке имитируется выключение и включение питания. Мы рекомендуем выполнять аппаратную перезагрузку, только если программная перезагрузка на дала требуемых результатов.

Чтобы выполнить аппаратную перезагрузку виртуальной сетевой функции или входящей в ее состав VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Выполните аппаратную перезагрузку виртуальной сетевой функции или входящей в ее состав VDU:

   - Если вы хотите выполнить аппаратную перезагрузку виртуальной сетевой функции, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** → **Аппаратная перезагрузка VNF**.

   - Если вы хотите выполнить аппаратную перезагрузку входящей в виртуальную сетевую функцию VDU, выполните следующие действия:

     1. Выберите вкладку **Управление VDU**.

        Отобразится таблица VDU.

     2. Нажмите на кнопку **Управление** → **Питание** → **Аппаратная перезагрузка VDU** рядом с VDU, аппаратную перезагрузку которой вы хотите выполнить.

5. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Будет выполнена аппаратная перезагрузка VNF или входящей в ее состав VDU.

Повторное развертывание виртуальной сетевой функции или входящей в ее состав VDU

Повторное развертывание виртуальной сетевой функции или входящей в ее состав VDU может привести к краткосрочным перебоям в ее работе или временной потере работоспособности. Мы рекомендуем планировать и координировать работы по повторному развертыванию в соответствии с требованиями вашей организации, чтобы свести нарушения работы к минимуму.

Чтобы повторно развернуть виртуальную сетевую функцию или входящую в ее состав VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Повторно разверните виртуальную сетевую функцию или входящую в ее состав VDU:

   - Если вы хотите повторно развернуть виртуальную сетевую функцию, в верхней части области настройки нажмите на кнопку **Управление** → **Повторно развернуть VNF**.

   - Если вы хотите повторно развернуть входящую в состав виртуальной сетевой функции VDU, выполните следующие действия:

     1. Выберите вкладку **Управление VDU**.

        Отобразится таблица VDU.

     2. Нажмите на кнопку **Управление** → **Повторно развернуть VDU** рядом с VDU, которую вы хотите повторно развернуть.

5. В открывшемся окне подтверждения нажмите на кнопку **Подтвердить**.

Начнется повторное развертывание виртуальной сетевой функции или входящей в ее состав VDU, которое может длиться несколько минут. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

Автоматическое восстановление виртуальной сетевой функции или входящей в ее состав VDU

Вы можете выполнить автоматическое восстановление виртуальной сетевой функции или входящей в ее состав VDU, даже если вы выключили автоматическое восстановление сетевого сервиса, в топологию которого добавлена виртуальная сетевая функция.

Чтобы автоматически восстановить виртуальную сетевую функцию или входящую в ее состав VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Выполните автоматическое восстановление виртуальной сетевой функции или входящей в ее состав VDU:

   - Если вы хотите выполнить автоматическое восстановление виртуальной сетевой функции, в верхней части области настройки нажмите на кнопку **Управление** → **Восстановление VNF**.

   - Если вы хотите выполнить автоматическое восстановление входящей в состав виртуальной сетевой функции VDU, выполните следующие действия:

     1. Выберите вкладку **Управление VDU**.

        Отобразится таблица VDU.

     2. Нажмите на кнопку **Управление** → **Восстановление VDU** рядом с VDU, автоматическое восстановление которой вы хотите выполнить.

5. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Начнется автоматическое восстановление виртуальной сетевой функции или входящей в ее состав VDU.

Работа с снимками состояния VDU

Для просмотра таблицы снимков состояния VDU вам нужно нажать на виртуальную сетевую функцию в топологии развернутого сетевого сервиса, выбрать вкладку **Управление VDU** и нажать на кнопку **Управление** → **Мгновенный снимок** рядом с VDU.

Информация о снимках состояния VDU отображается в следующих столбцах таблицы:

- **Имя** – имя снимка состояния VDU.
- **Дата создания** – дата и время создания снимка состояния VDU.
- **Размер** – размер снимка состояния VDU в байтах.
- **Описание** – краткое описание снимка состояния VDU.
- **Управление** – действия, которые можно выполнить с снимком состояния VDU.

Создание снимка состояния VDU

Мы не рекомендуем хранить снимки состояния в течение длительного времени, так как их наличие снижает производительность VDU.

Чтобы создать снимок состояния VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию, в состав которой входит VDU.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Питание** → **Мгновенный снимок** рядом с VDU, для которой вы хотите создать снимок состояния.

   Откроется окно с таблицей снимков состояния VDU.

6. В поле **Имя** введите имя снимка состояния VDU.

7. В поле **Описание** введите краткое описание снимка состояния VDU.

8. Нажмите на кнопку **Создать**.

Снимок состояния VDU будет создан и отобразится в таблице.

Восстановление параметров VDU с помощью снимка состояния

Чтобы восстановить параметры VDU с помощью снимка состояния:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию, в состав которой входит VDU.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Питание** → **Мгновенный снимок** рядом с VDU, параметры которой вы хотите восстановить с помощью снимка состояния.

   Откроется окно с таблицей снимков состояния VDU.

6. Нажмите на кнопку **Управление** → **Откатить** рядом с снимком состояния, с помощью которого вы хотите восстановить параметры VDU.

7. В открывшемся окне подтверждения нажмите на кнопку **Откатить**.

Параметры VDU будут восстановлены в соответствии со снимком состояния.

Изменение снимка состояния VDU

Чтобы изменить снимок состояния VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию, в состав которой входит VDU.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Питание** → **Мгновенный снимок** рядом с VDU, снимок состояния которой вы хотите изменить.

   Откроется окно с таблицей снимков состояния VDU.

6. Нажмите на кнопку **Управление** → **Изменить** рядом со снимком состояния VDU, который вы хотите изменить.

7. В открывшемся окне при необходимости измените имя и/или краткое описание снимка состояния VDU.

8. Нажмите на кнопку **Сохранить**.

Снимок состояния VDU будет изменен и обновится в таблице.

Удаление снимка состояния VDU

Удаленные снимки состояния VDU невозможно восстановить.

Чтобы удалить снимок состояния VDU:

1. На портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию, в состав которой входит VDU.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Питание** → **Мгновенный снимок** рядом с VDU, снимок состояния которой вы хотите удалить.

   Откроется окно с таблицей снимков состояния VDU.

6. Нажмите на кнопку **Управление** → **Удалить** рядом со снимком состояния VDU, который вы хотите удалить.

7. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Снимок состояния VDU будет удален и перестанет отображаться в таблице.

Работа с физическими сетевыми функциями

Для работы с физической сетевой функцией вам выполнить одно из следующих действий:

- на портале администратора перейти в раздел **Каталог** и в панели **Каталог** нажать на физическую сетевую функцию;
- при создании или изменении шаблона сетевого сервиса в топологии нажать на физическую сетевую функцию;
- при создании или изменении сетевого сервиса в топологии нажать на физическую сетевую функцию.

Параметры физической сетевой функции можно настроить на следующих вкладках:

- **Варианты развертывания** – варианты развертывания физической сетевой функции.
- **Параметры VNF** – основные параметры физической сетевой функции.

Следующие вкладки отображаются, если вы нажали на физическую сетевую функцию в топологии развернутого сетевого сервиса:

- **Мониторинг** – результаты мониторинга физической сетевой функции.
- **Проблемы** – проблемы, возникшие при работе физической сетевой функции. При наличии проблем рядом со вкладкой отображается красный восклицательный знак.

Дополнительно могут отображаться вкладки, которые вы указали в блоке `user_configurations` PNF-дескриптора.

Выбор варианта развертывания физической сетевой функции

Вы можете указать варианты развертывания в блоке `flavours` PNF-дескриптора.

Чтобы выбрать вариант развертывания физической сетевой функции:

1. Перейдите к топологии одним из следующих способов:
   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.
2. Нажмите на физическую сетевую функцию, вариант развертывания которой вы хотите выбрать.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.
3. Выберите вариант развертывания физической сетевой функции.
4. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры физической сетевой функции.

Настройка основных параметров физической сетевой функции

Чтобы настроить основные параметры физической сетевой функции:

1. Перейдите к топологии одним из следующих способов:
   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.
2. Нажмите на физическую сетевую функцию, основные параметры которой вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.
3. Выберите вкладку **Параметры PNF**.

   Отобразятся основные параметры физической сетевой функции.
4. В поле **Имя** введите имя физической сетевой функции.
5. В поле **Описание** введите краткое описание физической сетевой функции.

6. В поле **Порядок** введите порядковый номер развертывания физической сетевой функции. Когда вы развертываете сетевой сервис, физическая сетевая функция с наименьшим значением порядкового номера развертывается первой. Если в параметрах ни одной из добавленных в топологию физических сетевых функций не указан порядковый номер, все физические сетевые функции развертываются одновременно.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры физической сетевой функции.

Настройка P2P-сервиса

Чтобы настроить P2P-сервис:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.

2. Нажмите на P2P-сервис, который вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

3. В поле **Имя** введите имя P2P-сервиса.

4. При необходимости в поле **Описание** введите краткое описание P2P-сервиса.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры P2P-сервиса.

Настройка P2M-сервиса

Чтобы настроить P2M-сервис:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.

2. Нажмите на P2M-сервис, который вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

3. В поле **Имя** введите имя P2M-сервиса.

4. При необходимости в поле **Описание** введите краткое описание P2M-сервиса.

5. В поле **Точки подключения** введите максимальное количество точек подключения P2M-сервиса. Диапазон значений: от 2 до 9999. Если вы не указываете значение для этого параметра, количество точек подключения не ограничивается.

6. В раскрывающемся списке **Режим** выберите, используется ли в P2M-сервисе DFI (Default Forwarding Interface), на который отправляется неизвестный unicast-трафик:

   - **Классический** – не использовать DFI. Это значение выбрано по умолчанию.
   - **DFI с FIB на root и leafs** – использовать DFI на сервисном интерфейсе с ролью root.
   - **DFI с FIB на leaf** – использовать DFI на сервисном интерфейсе с ролью root. Вам нужно создать сервисные интерфейсы с ролью leaf на одном устройстве CPE. Резервные сервисные интерфейсы с ролью leaf требуется создать на одном устройстве CPE, отличном от устройства CPE, на котором созданы основные сервисные интерфейсы.

7. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. Значение по умолчанию: `300`.

8. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое применяется к серии кадров, когда первый кадр отправляется на контроллер для изучения MAC-адреса источника:

   - **Learn and flood** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отправляется на все добавленные в P2M-сервис сервисные интерфейсы, за исключением сервисного интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.
   - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отбрасывается.

   При наличии MAC-адреса назначения в MAC-таблице серия кадров отправляется на сервисный интерфейс назначения.

9. В поле **Размер MAC-таблицы** введите максимальное количество записей в MAC-таблице контроллера. Диапазон значений: от 0 до 65 535. Вы можете ввести `0`, чтобы не ограничивать количество записей. Значение по умолчанию: `100`.

10. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

    - **Flood** – трафик с неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.
    - **Drop** – трафик с неизученными MAC-адресами назначения не передается.

11. Если вы хотите настроить назначение IP-адресов виртуальным сетевым функциям с помощью DHCP, выполните следующие действия:

    a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**. Значение по умолчанию: **Выключить**.

    b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая назначает IP-адреса виртуальным сетевым функциям.

    c. Если вы хотите, чтобы подсеть OpenStack назначала виртуальным сетевым функциям указанный шлюз, в поле **Шлюз** введите IPv4-адрес шлюза.

    d. Укажите диапазон IP-адресов, из которого подсеть OpenStack назначает IP-адреса виртуальным сетевым функциям. Для этого в блоке **Пулы** нажмите на кнопку **+ Пул** и введите начальное и конечное значения диапазона IP-адресов.

    Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазоны IP-адресов. Для удаления диапазона IP-адресов нажмите рядом с ним на кнопку **Удалить**.

    e. Укажите DNS-сервер, который подсеть OpenStack назначает виртуальным сетевым функциям. Для этого в блоке **DNS** нажмите на кнопку **+ DNS** и введите IPv4-адрес DNS-сервера.

    DNS-сервер будет указан и отобразится в блоке **DNS**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на кнопку **Удалить**.

12. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры P2M-сервиса.

Настройка M2M-сервиса

Чтобы настроить M2M-сервис:

1. Перейдите к топологии одним из следующих способов:

    - Начните создание или изменение шаблона сетевого сервиса.
    - Начните создание или изменение сетевого сервиса.

2. Нажмите на M2M-сервис, который вы хотите настроить.

    Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

3. В поле **Имя** введите имя M2M-сервиса.

4. При необходимости в поле **Описание** введите краткое описание M2M-сервиса.

5. В поле **Точки подключения** введите максимальное количество точек подключения M2M-сервиса. Диапазон значений: от 2 до 9999. Если вы не указываете значение для этого параметра, количество точек подключения не ограничивается.

6. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. Значение по умолчанию: `300`.

7. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое применяется к серии кадров, когда первый кадр отправляется на контроллер для изучения MAC-адреса источника:

   - **Learn and flood** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отправляется на все добавленные в P2M-сервис сервисные интерфейсы, за исключением сервисного интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.

   - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отбрасывается.

   При наличии MAC-адреса назначения в MAC-таблице серия кадров отправляется на сервисный интерфейс назначения.

8. В поле **Размер MAC-таблицы** введите максимальное количество записей в MAC-таблице контроллера. Диапазон значений: от 0 до 65 535. Вы можете ввести `0`, чтобы не ограничивать количество записей. Значение по умолчанию: `100`.

9. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

   - **Flood** – трафик с неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.

   - **Drop** – трафик с неизученными MAC-адресами назначения не передается.

10. Если вы хотите настроить назначение IP-адресов виртуальным сетевым функциям с помощью DHCP, выполните следующие действия:

    a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**. Значение по умолчанию: **Выключить**.

    b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая назначает IP-адреса виртуальным сетевым функциям.

    c. Если вы хотите, чтобы подсеть OpenStack назначала виртуальным сетевым функциям указанный шлюз, в поле **Шлюз** введите IPv4-адрес шлюза.

    d. Укажите диапазон IP-адресов, из которого подсеть OpenStack назначает IP-адреса виртуальным сетевым функциям. Для этого в блоке **Пулы** нажмите на кнопку **+ Пул** и введите начальное и конечное значения диапазона IP-адресов.

       Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазоны IP-адресов. Для удаления диапазона IP-адресов нажмите рядом с ним на кнопку **Удалить**.

    e. Укажите DNS-сервер, который подсеть OpenStack назначает виртуальным сетевым функциям. Для этого в блоке **DNS** нажмите на кнопку **+ DNS** и введите IPv4-адрес DNS-сервера.

       DNS-сервер будет указан и отобразится в блоке **DNS**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на кнопку **Удалить**.

11. Если вы хотите использовать M2M-сервис для создания общего сетевого сервиса, установите флажок **Поделиться сетевым сервисом**. Этот флажок снят по умолчанию.

12. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры M2M-сервиса.

Настройка общей сети (OS 2 SHARED)

Чтобы настроить общую сеть в топологии:

1. Перейдите к топологии одним из следующих способов:
   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.
2. Нажмите на общую сеть, которую вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.
3. В поле **Имя** введите имя общей сети.
4. При необходимости в поле **Описание** введите краткое описание общей сети.
5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры общей сети.

Настройка виртуального маршрутизатора (OS vRouter)

Чтобы настроить виртуальный маршрутизатор:

1. Перейдите к топологии одним из следующих способов:
   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.
2. Нажмите на виртуальный маршрутизатор, который вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.
3. В поле **Имя** введите имя виртуального маршрутизатора.
4. При необходимости в поле **Описание** введите краткое описание виртуального маршрутизатора.
5. Если вы хотите выставить значение up для рабочего состояния виртуального маршрутизатора, установите флажок **Административное состояние**. Этот флажок снят по умолчанию.
6. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры виртуального маршрутизатора.

Настройка VLAN

Чтобы настроить VLAN:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.

2. В топологии нажмите на VLAN, которую вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

3. В поле **Имя** введите имя VLAN.

4. При необходимости в поле **Описание** введите краткое описание VLAN.

5. Если вы хотите настроить назначение IP-адресов виртуальным сетевым функциям с помощью DHCP, выполните следующие действия:

   a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**. Значение по умолчанию: **Выключить**.

   b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая назначает IP-адреса виртуальным сетевым функциям.

   c. Если вы хотите, чтобы подсеть OpenStack назначала виртуальным сетевым функциям указанный шлюз, в поле **Шлюз** введите IPv4-адрес шлюза.

   d. Укажите диапазон IP-адресов, из которого подсеть OpenStack назначает IP-адреса виртуальным сетевым функциям. Для этого в блоке **Пулы** нажмите на кнопку **+ Пул** и введите начальное и конечное значения диапазона IP-адресов.

      Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазоны IP-адресов. Для удаления диапазона IP-адресов нажмите рядом с ним на кнопку **Удалить**.

   e. Укажите DNS-сервер, который подсеть OpenStack назначает виртуальным сетевым функциям. Для этого в блоке **DNS** нажмите на кнопку **+ DNS** и введите IPv4-адрес DNS-сервера.

      DNS-сервер будет указан и отобразится в блоке **DNS**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на кнопку **Удалить**.

6. Если вы хотите использовать VLAN для создания общего сетевого сервиса, установите флажок **Поделиться сетью**. Этот флажок снят по умолчанию.

7. Если вы хотите назначать виртуальным сетевым функциям VLAN-тег, в поле **ID сегментации** введите VLAN-тег.

8. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры VLAN.

Настройка VXLAN

Чтобы настроить VXLAN:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.

2. Нажмите на VXLAN, которую вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

3. В поле **Имя** введите имя VXLAN.

4. При необходимости в поле **Описание** введите краткое описание VXLAN.

5. Если вы хотите настроить назначение IP-адресов виртуальным сетевым функциям с помощью DHCP, выполните следующие действия:

   a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**. Значение по умолчанию: **Выключить**.

   b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая назначает IP-адреса виртуальным сетевым функциям.

   c. Если вы хотите, чтобы подсеть OpenStack назначала виртуальным сетевым функциям указанный шлюз, в поле **Шлюз** введите IPv4-адрес шлюза.

   d. Укажите диапазон IP-адресов, из которого подсеть OpenStack назначает IP-адреса виртуальным сетевым функциям. Для этого в блоке **Пулы** нажмите на кнопку **+ Пул** и введите начальное и конечное значения диапазона IP-адресов.

      Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазоны IP-адресов. Для удаления диапазона IP-адресов нажмите рядом с ним на кнопку **Удалить**.

   e. Укажите DNS-сервер, который подсеть OpenStack назначает виртуальным сетевым функциям. Для этого в блоке **DNS** нажмите на кнопку **+ DNS** и введите IPv4-адрес DNS-сервера.

      DNS-сервер будет указан и отобразится в блоке **DNS**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на кнопку **Удалить**.

6. Если вы хотите использовать VXLAN для создания общего сетевого сервиса, установите флажок **Поделиться сетью**. Этот флажок снят по умолчанию.

7. Если вы хотите назначать виртуальным сетевым функциям VXLAN-тег, в поле **ID сегментации** введите VXLAN-тег.

8. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры VXLAN.

Настройка плоской сети

Чтобы настроить плоскую сеть:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.

2. Нажмите на плоскую сеть, которую вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

3. В поле **Имя** введите имя плоской сети.

4. При необходимости в поле **Описание** введите краткое описание плоской сети.

5. Если вы хотите настроить назначение IP-адресов виртуальным сетевым функциям с помощью DHCP, выполните следующие действия:

   a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**. Значение по умолчанию: **Выключить**.

   b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая назначает IP-адреса виртуальным сетевым функциям.

   c. Если вы хотите, чтобы подсеть OpenStack назначала виртуальным сетевым функциям указанный шлюз, в поле **Шлюз** введите IPv4-адрес шлюза.

   d. Укажите диапазон IP-адресов, из которого подсеть OpenStack назначает IP-адреса виртуальным сетевым функциям. Для этого в блоке **Пулы** нажмите на кнопку **+ Пул** и введите начальное и конечное значения диапазона IP-адресов.

      Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазоны IP-адресов. Для удаления диапазона IP-адресов нажмите рядом с ним на кнопку **Удалить**.

   e. Укажите DNS-сервер, который подсеть OpenStack назначает виртуальным сетевым функциям. Для этого в блоке **DNS** нажмите на кнопку **+ DNS** и введите IPv4-адрес DNS-сервера.

      DNS-сервер будет указан и отобразится в блоке **DNS**. Вы можете указать несколько DNS-серверов и удалить DNS-серверы. Для удаления DNS-сервера нажмите рядом с ним на кнопку **Удалить**.

6. Если вы хотите использовать плоскую сеть для создания общего сетевого сервиса, установите флажок **Поделиться сетью**. Этот флажок снят по умолчанию.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры плоской сети.

Настройка UNI

Чтобы настроить UNI:

1. Перейдите к топологии одним из следующих способов:

   - Начните создание или изменение шаблона сетевого сервиса.
   - Начните создание или изменение сетевого сервиса.

2. Нажмите на UNI, который вы хотите настроить.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗.

3. В поле **Имя** введите имя UNI.

4. При необходимости в поле **Описание** введите краткое описание UNI.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры UNI.

Мониторинг компонентов решения

Мониторинг устройств CPE, а также виртуальных сетевых функций и физических сетевых функций обеспечивается внешней системой мониторинга Zabbix. Вам нужно развернуть сервер Zabbix на одной из ваших площадок, либо подключить уже имеющийся сервер Zabbix, а также развернуть серверы Zabbix-прокси.

Серверы Zabbix-прокси используются для получения результатов мониторинга на отдельных площадках и отправки результатов мониторинга на сервер Zabbix. Сервер Zabbix обрабатывает результаты мониторинга, после чего они отображаются в веб-интерфейсе оркестратора.

Оркестратор интегрируется с сервером Zabbix с помощью API. Когда вы регистрируете устройство CPE, а также развертываете виртуальную сетевую функцию или физическую сетевую функцию в сетевом сервисе, на сервере Zabbix автоматически создается соответствующий хост. Вы можете указать, в какие группы на сервере Zabbix помещаются хосты. Хост на сервере Zabbix автоматически удаляется, если вы удаляете соответствующее ему устройство CPE, а также виртуальную сетевую функцию или физическую сетевую функцию.

Поддерживается два способа мониторинга:

- Мониторинг с помощью Zabbix-агентов – компонент автоматически передает данные мониторинга серверу Zabbix-прокси.
- Мониторинг с помощью протокола SNMP – сервер Zabbix-прокси автоматически подключается к компоненту по протоколу SNMP и получает данные мониторинга.

Более подробную информацию о настройке системы мониторинга можно получить из официальной документации решения Zabbix.

Указание сервера Zabbix

Чтобы указать сервер Zabbix:

1. В меню перейдите в раздел **Система**.

   По умолчанию выбрана вкладка **Мониторинг**, на которой отображаются параметры подключения к серверу Zabbix.

2. Выберите вкладку **Мониторинг**.

   Отобразятся параметры подключения к серверу Zabbix.

3. В поле **URL** введите веб-адрес Zabbix API. Оркестратор отправляет на введенный веб-адрес HTTP-запросы для получения и отображения результатов мониторинга в виде графиков.

   Веб-адрес состоит из адреса веб-интерфейса Zabbix и имени файла api_jsonrpc.php, который используется для вызова API. Например, если веб-интерфейс Zabbix расположен по адресу http://192.168.2.1, вам нужно ввести `http://192.168.2.1/api_jsonrpc.php`.

4. В поле **Имя пользователя** введите имя пользователя для подключения оркестратора к Zabbix API. Вам нужно ввести имя пользователя для учетной записи, имеющей права на чтение и запись в группах на сервере Zabbix, а также права на создание групп.

5. В поле **Пароль** введите пароль пользователя для подключения к Zabbix API.

6. В раскрывающемся списке **Группировка по Zabbix** выберите способ группировки хостов устройств CPE, а также виртуальных сетевых функций и физических сетевых функций на сервере Zabbix:

   - **По указанным группам** – помещать хосты устройств CPE, а также виртуальных сетевых функций и физических сетевых функций в указанные группы. При выборе этого значения выполните следующие действия:

     a. В поле **VNF/PNF-группа** введите имя группы для хостов виртуальных сетевых функций и физических сетевых функций.

     b. В поле **Группа CPE** введите имя группы для хостов устройств CPE.

   - **По тенанту** – помещать хосты устройств CPE, а также виртуальных сетевых функций и физических сетевых функций в автоматически созданные группы. Группы соответствуют тенантам, которым добавлены устройства CPE, а также назначены виртуальные сетевые функции и физические сетевые функции.

7. В поле **Синхронизация триггеров (сек.)** введите интервал времени в секундах для получения оркестратором уведомлений о возникших проблемах от сервера Zabbix. Диапазон значений: от 5 до 600. Значение по умолчанию: `600`.

8. Снизу от поля **Токен** нажмите на кнопку **Сгенерировать**, чтобы сгенерировать токен, который содержат API-запросы сервера Zabbix к оркестратору. Если API-запрос не содержит токен, оркестратор не принимает API-запрос. Безопасность также обеспечивается TLS-сертификатами.

   Вы можете ввести токен вручную, а также посмотреть его, нажав на значок просмотра 👁.

9. Если вы хотите проверить доступность сервера Zabbix, нажмите на кнопку **Проверить соединение**.

10. Нажмите на кнопку **Применить**.

    Сервер Zabbix будет указан.

Указание сервера Zabbix-прокси

Чтобы указать сервер Zabbix-прокси:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. В панели **Ресурсы** выберите созданный домен, после чего выберите добавленный центр обработки данных, для которого вы хотите указать сервер Zabbix-прокси.

3. Выберите вкладку **Системные ресурсы**.

   Отобразятся параметры подключения к серверу Zabbix-прокси и VNFM.

4. В блоке **Zabbix-прокси** в поле **Имя** введите имя сервера Zabbix-прокси. Введенное имя должно совпадать с именем, указанным в параметрах сервера Zabbix.

5. В поле **IP** введите IP-адрес сервера Zabbix-прокси. Введенный IP-адрес должен быть доступен для устройств CPE, а также виртуальных сетевых функций и физических сетевых функций, мониторинг которых вы хотите обеспечить.

6. Нажмите на кнопку **Применить**

Сервер Zabbix-прокси будет указан.

Вы можете удалить параметры подключения к серверу Zabbix-прокси, нажав на кнопку **Удалить**.

Настройка мониторинга устройств CPE

Вы можете настроить мониторинг в шаблоне CPE. Параметры мониторинга, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

Чтобы настроить мониторинг устройств CPE:

1. В меню перейдите в раздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, в котором вы хотите настроить мониторинг.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Мониторинг**.

   Отобразятся параметры мониторинга устройства CPE.

4. В раскрывающемся списке **Тип мониторинга** выберите способ мониторинга устройства CPE:

   - **SNMP** – мониторинг с помощью протокола SNMP.
   - **Agent** – мониторинг с помощью Zabbix-агентов.

5. В поле **Шаблон Zabbix** введите имя шаблона Zabbix.

6. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE.

Просмотр результатов мониторинга

Вы можете посмотреть результаты мониторинга экземпляра SD-WAN, устройства CPE, а также виртуальной сетевой функции и физической сетевой функции:

- Для просмотра результатов мониторинга экземпляра SD-WAN вам нужно в меню перейти в раздел **SD-WAN → Экземпляры SD-WAN**, нажать на экземпляр SD-WAN и выбрать вкладку **Мониторинг**.
- Для просмотра результатов мониторинга устройства CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Мониторинг**.
- Для просмотра результатов мониторинга виртуальной сетевой функции или физической сетевой функции вам нужно войти на портал самообслуживания, в меню перейти в раздел **Каталог**, в панели **Сетевые сервисы** нажать на развернутый сетевой сервис, нажать на виртуальную или физическую сетевую функцию и выбрать вкладку **Мониторинг**.

Вы можете выбрать параметр, для которого отображаются результаты мониторинга, с помощью раскрывающегося списка в верхней части области настройки. Для просмотра результатов мониторинга за выбранный период вам нужно использовать следующие фильтры времени:

- **В реальном времени**.
- **День**.
- **Неделя**.
- **Месяц**.

Период времени можно указать вручную.

Просмотр проблем

Параметры мониторинга на сервере Zabbix определяют, о каких проблемах требуется отправлять уведомления и как проблемы классифицируются по уровням критичности. Вы можете посмотреть таблицу проблем на устройстве CPE, а также в параметрах виртуальной и физической сетевой функции:

- Для просмотра таблицы проблем на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Проблемы**.
- Для просмотра таблицы проблем в параметрах виртуальной или физической сетевой функции вам нужно войти на портал самообслуживания, в меню перейти в раздел **Каталог**, в панели **Сетевые сервисы** нажать на развернутый сетевой сервис, нажать на виртуальную сетевую функцию или физическую сетевую функцию и выбрать вкладку **Проблемы**.

Информация о проблемах отображается в следующих столбцах таблицы:

- **Имя** – имя проблемы.
- **Уровень** – уровень критичности проблемы:
  - **Average**.
  - **Disaster**
  - **High**.
  - **Information**.
  - **Not classified**.
- **Время** – время возникновения проблемы.
- **Продолжительность** – продолжительность проблемы в секундах.

Просмотр состояния решения и его компонентов

Чтобы посмотреть состояние компонентов решения,

1. В меню перейдите в раздел **Обозреватель**.

   Отобразятся следующие блоки с информацией:

   - **Ошибки в событиях** – ошибки, возникшие при выполнении событий.
   - **Ошибки в задачах** – ошибки, возникшие при выполнении пользовательских задач.
   - **Активные сеансы** – активные пользовательские сеансы.
   - **Ресурсы** – информация об использовании вычислительных ресурсов компонентами решения.
   - **Сервисные запросы** – сервисные запросы.
   - **Отключенные CPE** – устройства CPE, доступ к которым был потерян.
   - **Ошибки в статусе CPE** – ошибки, возникшие при работе устройств CPE.
   - **Проблемы на CPE** – проблемы, возникшие при работе устройств CPE.
   - **Проблемы на VNF/PNF** – проблемы, возникшие при работе виртуальных сетевых функций и физических сетевых функций.

   Если компонент решения работает правильно, в соответствующем блоке отображается сообщение *Все работает правильно*. В верхней части блоков отображается значок обновления, при нажатии на который обновляется отображаемая информация. Вы можете перетаскивать блоки мышью для изменения порядка их отображения.

2. Если вы хотите установить отображение блоков по умолчанию, в верхней части страницы нажмите на значок настройки → **Сбросить до макета по умолчанию**.

3. Если вы хотите изменить интервал времени для обновления информации в блоках, выполните следующие действия:

   a. В верхней части страницы нажмите на значок настройки → **Установить интервал обновления**.

   b. В открывшемся окне в поле **Обновлять панель каждые (сек.)** введите интервал времени в секундах для обновления информации в блоках. Диапазон значений: от 5 до 86 400. По умолчанию. указано значение `60`.

   c. Нажмите на кнопку **Ок**.

   Интервал времени для обновления информации в блоках будет изменен.

Просмотр журналов

Вы можете посмотреть журналы работы компонентов решения для осуществления технической поддержки. Kaspersky SD-WAN не отправляет журналы за пределы периметра информационной инфраструктуры вашей организации.

Чтобы посмотреть журналы:

1. В меню перейдите в раздел **Журналы**.

   Откроется страница управления журналами.

2. В панели **Центры обработки данных** выберите созданный центр обработки данных, к которому относятся компоненты решения.

3. В панели **Ресурсы** выберите компонент решения, журнал которого вы хотите посмотреть.

   Отобразится журнал. По умолчанию выбрана вкладка **Задачи**, на которой отображается таблица пользовательских задач. Информация о пользовательских задачах отображается в следующих столбцах таблицы:

   - **Действие задачи** – действие пользовательской задачи.
   - **Объект** – компонент решения, связанный с пользовательской задачей.
   - **СЗ** – ссылка на сервисный запрос, связанный с пользовательской задачей.
   - **ID объекта** – идентификатор компонента решения, связанного с пользовательской задачей.
   - **Имя объекта** – имя компонента решения, связанного с пользовательской задачей.
   - **Инициатор** – имя пользователя, выполнившего пользовательскую задачу.
   - **IP инициатора** – IP-адрес пользователя, выполнившего пользовательскую задачу.
   - **Время начала** – дата и время начала выполнения пользовательской задачи.
   - **Время окончания** – дата и время окончания выполнения пользовательской задачи.

4. Если вы хотите посмотреть информацию о событиях, возникших при работе компонента решения, выберите вкладку **События**.

   Отобразится таблица событий. Информация о событиях отображается в следующих столбцах таблицы:

   - **Действие события** – действие события.
   - **Объект** – компонент решения, связанный с событием.
   - **СЗ** – ссылка на сервисный запрос, связанный с событием.
   - **Имя объекта** – имя компонента решения, связанного с событием.
   - **ID объекта** – идентификатор компонента решения, связанного с событием.
   - **Инициатор** – имя пользователя, действие которого привело к созданию события.
   - **Время** – дата и время создания события.

5. Если вы хотите посмотреть сервисные запросы компонента решения, выберите вкладку **Сервисные запросы**.

   Отобразится таблица сервисных запросов. Информация о сервисных запросах отображается в следующих столбцах таблицы:

   - **Сервисный запрос** – имя сервисного запроса.
   - **Статус** – статус сервисного запроса.
   - **Инициатор** – имя пользователя, действие которого привело к созданию сервисного запроса.
   - **Время** – дата и время создания сервисного запроса.

Действия, которые вы можете выполнить с таблицами, описаны в инструкции Работа с таблицами компонентов решения.

Просмотр и удаление сервисных запросов

Сервисные запросы (англ. service requests) – это задачи, которые выполняются при работе компонентов решения и создаются автоматически в результате действий пользователей. Например, когда пользователь применяет шаблон CPE к устройству CPE, создается соответствующий сервисный запрос. Каждый сервисный запрос состоит из нескольких шагов, которые выполняются поочередно.

Просмотр сервисных запросов

Вы можете посмотреть сервисные запросы тенанта, устройства CPE и экземпляра SD-WAN:

- Для просмотра сервисных запросов тенанта вам нужно в меню перейти в раздел **Тенанты** и в блоке **Тенанты** выбрать тенанта.

  Список сервисных запросов отобразится в блоке **Сервисные запросы**.

- Для просмотра сервисных запросов экземпляра SD-WAN вам нужно в меню перейти в раздел **SD-WAN** → **Экземпляры SD-WAN**, нажать на экземпляр SD-WAN и выбрать вкладку **Сервисные запросы**.

  Отобразится таблица сервисных запросов.

- Для просмотра сервисных запросов устройства CPE вам нужно в меню перейти в раздел **SD-WAN** → **CPE**, нажать на устройство CPE и выбрать вкладку **Сервисные запросы**.

  Отобразится таблица сервисных запросов.

В списке сервисных запросов тенанта отображается имя и идентификатор сервисного запроса, а также дата и время его создания. Информация о сервисных запросах экземпляра SD-WAN и устройства CPE отображается в следующих столбцах таблицы:

- **Имя** – имя сервисного запроса.
- **Создан** – дата и время создания сервисного запроса.
- **ID задачи** – идентификатор сервисного запроса.
- **Время** – продолжительность сервисного запроса в секундах.
- **Статус** – статус сервисного запроса:
  - **Выполнение** – сервисный запрос выполняется.
  - **Не выполнен** – при выполнении сервисного запроса произошла ошибка.
  - **Выполнен** – сервисный запрос успешно выполнен.
  - **Отменяется** – при выполнении одного из шагов сервисного запроса произошла ошибка, поэтому отменяются ранее выполненные шаги.
  - **Не отменен** – при отмене одного из ранее выполненных шагов сервисного запроса произошла ошибка.
  - **Отменен** – ранее выполненные шаги сервисного запроса успешно отменены.
  - **Приостановлен** – при выполнении сервисного запроса на регистрацию устройства CPE произошла ошибка, и регистрация устройства CPE не была завершена. Вы можете возобновить регистрацию устройства CPE.
- **Действия** – действия, которые можно выполнить с сервисным запросом.

Вы можете открыть журнал выполнения сервисного запроса:

- Если вы хотите открыть журнал выполнения сервисного запроса тенанта, нажмите на имя сервисного запроса.
- Если вы хотите открыть журнал выполнения сервисного запроса экземпляра SD-WAN или устройства CPE, нажмите на идентификатор сервисного запроса.

Откроется журнал выполнения сервисного запроса.

Журнал содержит информацию о шагах, на которых произошли ошибки. Вы можете нажать на шаг, на котором произошла ошибка, чтобы посмотреть подробное описание ошибки.

Удаление сервисных запросов

Вы можете удалить сервисные запросы экземпляра SD-WAN и устройства CPE. При этом будут удалены только сервисные запросы, имеющие статус, отличный от **Приостановлено**. При удалении сервисного запроса прекращается выполнение связанной с ним операции.

Удаленные сервисные запросы невозможно восстановить.

Для удаления сервисного запроса вам нужно выполнить одно из следующих действий:

- Если вы хотите удалить отдельный сервисный запрос, нажмите рядом с ним на кнопку **Удалить**.
- Если вы хотите удалить все сервисные запросы, в верхней части области настройки в блоке **Действия** нажмите на кнопку **Удалить все**.

Подтвердите удаление, нажав на кнопку **Удалить** в открывшемся окне.

Сервисные запросы будут удалены и перестанут отображаться в таблице.

Отправка уведомлений об устройствах CPE пользователям

Kaspersky SD-WAN поддерживает отправку уведомлений со следующей информацией об устройствах CPE на электронную почту пользователей:

- События из журнала:
  - включение или выключение устройства CPE;
  - подключение или отключение порта;
  - подключение или отключение соединения.
- Проблемы:
  - возникшие проблемы;
  - разрешенные проблемы.

Информация накапливается в течение пяти секунд перед отправкой уведомления. Например, если отключение порта приводит к отключению пяти соединений, эту информацию необходимо накопить и отправить пользователю в одном уведомлении.

Вам нужно указать SMTP-сервер, который будет использоваться всеми тенантами для отправки уведомлений. На портале администратора вы можете настроить отправку уведомлений о событиях и проблемах всех тенантов. На портале самообслуживания вы можете настроить отправку уведомлений о событиях и проблемах отдельного тенанта.

Указание SMTP-сервера

Чтобы указать SMTP-сервер:

1. В меню перейдите в раздел **Система**.

   По умолчанию выбрана вкладка **Мониторинг**, на которой отображаются параметры подключения к серверу Zabbix.

2. Выберите вкладку **Оповещения** → **SMTP**.

   Отобразятся параметры подключения к SMTP-серверу.

3. Установите флажок **Включить**, чтобы использовать SMTP-сервер. Этот флажок снят по умолчанию.

4. В поле **SMTP-сервер** введите IP-адрес или доменное имя SMTP-сервера.

5. В поле **Порт SMTP-сервера** введите номер порта SMTP-сервера. Диапазон значений: от 0 до 65 535. Значение по умолчанию: `25`.

6. В поле **Эл. почта отправителя** введите адрес электронной почты, с которого SMTP-сервер отправляет уведомления пользователям.

7. Если вы хотите настроить шифрование соединения между Kaspersky SD-WAN и SMTP-сервером, в раскрывающемся списке **SSL/TLS** выберите одно из следующих значений:

   - **Отсутствует** – не шифровать соединение. Это значение выбрано по умолчанию.
   - **STARTTLS** – определить метод шифрования, после чего установить зашифрованное соединение.
   - **SMTPS** – изначально установить зашифрованное соединение.

8. Если вы хотите включить аутентификацию Kaspersky SD-WAN в SMTP-сервере, выполните следующие действия:

   a. Установите флажок **Аутентификация**. Этот флажок снят по умолчанию.

   b. В поле **Имя пользователя** введите имя пользователя, которое Kaspersky SD-WAN использует при аутентификации в SMTP-сервере. Максимальная длина имени: 64 символа.

   c. В поле **Пароль** введите пароль, который Kaspersky SD-WAN использует при аутентификации в SMTP-сервере. Максимальная длина пароля: 64 символа. Вы можете просмотреть введенный пароль, нажав на значок просмотра 👁.

9. Если вы хотите отправить тестовое сообщение с помощью SMTP-сервера, выполните следующие действия:

   a. Нажмите на кнопку **Тест**.

   b. В открывшемся окне введите адрес электронной почты, на который SMTP-сервер отправляет тестовое сообщение.

   c. Нажмите на кнопку **Отправить**.

   На указанный адрес электронной почты будет отправлено тестовое сообщение, в теме и тексте которого будет указано *Notification test*.

10. Нажмите на кнопку **Применить**.

SMTP-сервер будет указан.

Настройка отправки уведомлений

Администратору платформы нужно указать SMTP-сервер для отправки уведомлений пользователю.

Чтобы настроить отправку уведомлений:

1. В меню перейдите в раздел **Система**.

   По умолчанию выбрана вкладка **Мониторинг**, на которой отображаются параметры подключения к серверу Zabbix.

2. Выберите вкладку **Оповещения → Предупреждение**.

   Отобразятся параметры отправки уведомлений.

3. Установите флажок **Включить**, чтобы отправлять уведомления пользователю. Этот флажок снят по умолчанию.

4. В поле **Адресат** введите адрес электронной почты, на который вы хотите отправлять уведомления.

5. В поле **Тема** введите текст темы электронных писем с уведомлениями. Максимальная длина темы: 64 символа.

6. Нажмите на кнопку **Применить**.

Уведомления будут отправляться на указанный адрес электронной почты.

Выбор уровня детализации журналов Docker-контейнеров

Kaspersky SD-WAN автоматически ведет журналы Docker-контейнеров контроллера и оркестратора. Вы можете выбрать уровень детализации журналов Docker-контейнеров.

Чтобы выбрать уровень детализации журналов Docker-контейнеров:

1. Перейдите к выбору уровня детализации журналов Docker-контейнеров одним из следующих способов:

   - Если вы хотите выбрать уровень детализации журналов Docker-контейнеров контроллера, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейдите в раздел **Журналы**.

   - Если вы хотите выбрать уровень детализации журналов Docker-контейнеров оркестратора, в меню перейдите в раздел **Система** и выберите вкладку **Журнал оркестратора**.

   Откроется страница, на которой отображается таблица Docker-контейнеров. Информация о Docker-контейнерах отображается в следующих столбцах таблицы:

   - **Имя модуля** – имя Docker-контейнера.

   - **Уровень журналирования** – уровень детализации журналов Docker-контейнера.

   Вы можете найти Docker-контейнер, введя его имя в поле **Фильтр**.

2. Выберите уровень детализации журналов Docker-контейнеров одним из следующих способов:

   - Если вы хотите выбрать уровень детализации журналов всех Docker-контейнеров, в блоке **Общий уровень журналирования** нажмите на соответствующую кнопку.

   - Если вы хотите выбрать уровень детализации журналов отдельного Docker-контейнера, нажмите рядом с ним на соответствующую кнопку.

   Вы можете выбрать следующие уровни детализации Docker-контейнеров:

   - **ТРАССИРОВКА** – включить в журнал наиболее полную информацию о работе и состоянии модуля и его переменных. Вы можете использовать этот уровень детализации для отслеживания процесса выполнения кода, а также диагностики и детального анализа возникших при разработке ошибок.

   - **ОТЛАДКА** – включить в журнал информацию, необходимую для отладки модуля, например состояние выполнения операций и значения переменных. Вы можете использовать этот уровень детализации для диагностики ошибок и анализа поведения модуля.

   - **ИНФОРМАЦИЯ** – включить в журнал общую информацию, необходимую для понимания работы модуля, например подтверждения выполнения операций. Вы можете использовать этот уровень детализации для отслеживания хода выполнения модуля. Этот уровень детализации выбран по умолчанию для всех контейнеров.

   - **ПРЕДУПРЕЖДЕНИЕ** – включить в журнал информацию о происшествиях, которые не являются ошибками, но могут скомпрометировать работу контейнера и требуют вашего вмешательства, например проблемы в параметрах и устаревшие функции. Вы можете использовать этот уровень детализации для предотвращения потенциальных ошибок.

   - **ОШИБКА** – включить в журнал информацию об ошибках, которые возникли при выполнении кода и требуют вашего вмешательства. Сообщение об ошибке может содержать информацию о части контейнера, в которой произошла ошибка, а также подробную информацию об ошибке. Вы можете использовать этот уровень детализации для устранения возникших ошибок.

Уровень детализации журналов Docker-контейнеров будет изменен.

Мониторинг устройств CPE, VNF и PNF с помощью протокола SNMP

Вы можете использовать протокол SNMP для мониторинга устройств CPE, а также виртуальных сетевых функций и физических сетевых функций. Вам нужно установить SNMP-агент на компонент, мониторинг которого вы хотите обеспечить. SNMP-агент получает данные мониторинга и передает их SNMP-менеджеру для обработки. В Kaspersky SD-WAN в роли SNMP-менеджера выступает сервер Zabbix-прокси.

SNMP-менеджер и SNMP-агенты обмениваются запросами и уведомлениями. По умолчанию SNMP-агенты получают запросы от SNMP-менеджера через порт 161. При этом SNMP-менеджер может отправлять запросы через любой доступный порт. Ответ приходит на тот же порт, с которого был отправлен запрос.

По умолчанию SNMP-менеджер получает уведомления от SNMP-агентов через порт 162. При этом SNMP-агенты могут отправлять уведомления через любые доступные порты. Существует два типа уведомлений:

- *Уведомления-ловушки* (англ. traps) – это уведомления о событиях, которые SNMP-агент отправляет без предварительного запроса от SNMP-менеджера. При возникновении указанного вами события, например выключения устройства CPE или одного из его сетевых интерфейсов, SNMP-агент генерирует уведомление-ловушку и отправляет его SNMP-менеджеру в виде UPD-сообщения. Уведомления-ловушки позволяют автоматически информировать SNMP-менеджер о возникновении событий, не дожидаясь получения запроса.

- *Запрос на информирование* (англ. inform request) – это похожие на уведомления-ловушки уведомления, которые отличаются тем, что требуют дополнительного подтверждения со стороны SNMP-менеджера. Когда SNMP-агент отправляет SNMP-менеджеру запрос на информирование, SNMP-агент ожидает получения подтверждения приема. Если SNMP-менеджер успешно принимает и обрабатывает запрос на информирование, он отправляет сообщение с подтверждением SNMP-агенту. Механизм подтверждения приема позволяет убедиться в надежности доставки уведомлений.

При использовании протокола TLS или DTLS уведомления-ловушки приходят на порт 10162 SNMP-менеджера, а запросы на информирование – на порт 10161.

Все основные протокольные единицы данных (англ. protocol data unit, PDU) имеют одинаковую структуру (см. рисунок ниже). IP-заголовок и UDP-заголовок используются для инкапсуляции и фактически не являются частями протокольной единицы данных.

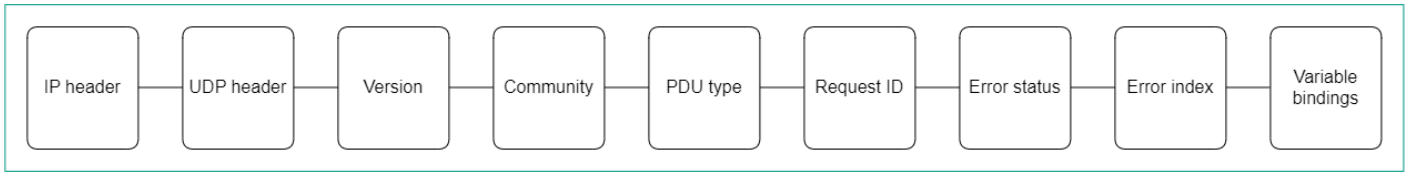


Схема единицы данных протокола SNMP

Для просмотра таблицы уведомлений-ловушек вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, к которому подключены компоненты для мониторинга, и перейти в раздел **SNMP**. Информация об уведомления-ловушках отображается в следующих столбцах таблицы:

- **#** – порядковый номер уведомления-ловушки.

- **IP менеджера** – IP-адрес или имя хоста SNMP-менеджера.

- **Порт менеджера** – номер порта SNMP-менеджера.
- **Сообщество** – строка сообщества SNMP.
- **Разрешенные ловушки** – уведомления-ловушки, которые SNMP-агенты отправляет SNMP-менеджеру.
- **Описание** – краткое описание уведомления-ловушки.

Настройка подключения SNMP-менеджера к SNMP-агентам

Вам нужно указать параметры подключения SNMP-менеджера к SNMP-агентам, установленным на устройствах CPE, а также на виртуальных сетевых функциях и физических сетевых функциях. Указанные параметры используются для всех SNMP-агентов.

Чтобы настроить подключение SNMP-менеджера к SNMP-агентам:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, к которому подключены компоненты для мониторинга.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **SNMP**.

   Отобразится таблица уведомлений-ловушек.

4. В верхней части страницы в блоке **Параметры менеджера** нажмите на кнопку **Изменить**.

5. В открывшемся окне в поле **Адрес** введите IP-адрес или имя хоста компонента, на котором установлен SNMP-агент, в формате `<транспортный протокол>:<IP-адрес или имя хоста>/<номер порта>`. Например, вы можете ввести `udp:192.168.2.0/24`.

6. В поле **Сообщество** введите строку сообщества SNMP (англ. SNMP community string). Строка сообщества SNMP используется как пароль, с помощью которого SNMP-менеджер подключается к SNMP-агентам. Значение по умолчанию: `public` – доступ предоставлен только для чтения. Мы рекомендуем изменить значение по умолчанию на уникальную строку сообщества, чтобы обеспечить безопасность взаимодействия между SNMP-менеджером и SNMP-агентами.

   > Вам нужно указать одинаковую строку сообщества при настройке подключения SNMP-менеджера к SNMP-агентам, а также при создании и изменении уведомлений-ловушек.

7. Нажмите на кнопку **Сохранить**.

Параметры подключения SNMP-менеджера к агентам будут указаны.

Создание уведомления-ловушки

Вы можете создать уведомление-ловушку, которое SNMP-агенты будут отправлять SNMP-менеджеру.

Чтобы создать уведомление-ловушку:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, к которому подключены компоненты для мониторинга.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **SNMP**.

   Отобразится таблица уведомлений-ловушек.

4. В блоке **Параметры ловушки** нажмите на кнопку **Изменить**.

5. В открывшемся окне нажмите на кнопку **+ Добавить**, чтобы создать уведомление-ловушку.

6. В поле **IP менеджера** введите IP-адрес или имя хоста SNMP-менеджера. Диапазон значений: от 1 до 255.

7. В поле **Порт менеджера** введите номер порта SNMP-менеджера. Диапазон значений: от 1 до 65 534. Значение по умолчанию: `162`.

8. В поле **Сообщество** введите строку сообщества SNMP. Строка сообщества SNMP используется как пароль, с помощью которого SNMP-менеджер подключается к SNMP-агентам. Значение по умолчанию: `public` – доступ предоставлен только для чтения. Мы рекомендуем изменить значение по умолчанию на уникальную строку сообщества, чтобы обеспечить безопасность взаимодействия между SNMP-менеджером и SNMP-агентами.

   Вам нужно указать одинаковую строку сообщества SNMP при настройке подключения SNMP-менеджера к SNMP-агентам, а также при создании и изменении уведомлений-ловушек.

9. В поле **Разрешенные ловушки** нажмите на кнопку **Изменить** и снимите следующие флажки, чтобы выбрать, какие уведомления-ловушки SNMP-агенты не отправляют SNMP-менеджеру:

   - Снимите флажок **Ловушка, когда интерфейс активен**, чтобы SNMP-агент не отправлял SNMP-менеджеру уведомление-ловушку, когда один из портов компонента, на котором установлен SNMP-агент, переходит в активное состояние.
   - Снимите флажок **Ловушка, когда интерфейс неактивен**, чтобы SNMP-агент не отправлял SNMP-менеджеру уведомление-ловушку, когда один из портов компонента, на котором установлен SNMP-агент, переходит в неактивное состояние.
   - Снимите флажок **Ловушка, когда оборудование активно**, чтобы SNMP-агент не отправлял SNMP-менеджеру уведомление-ловушку, когда компонент, на котором установлен SNMP-агент, переходит в активное состояние.
   - Снимите флажок **Ловушка, когда оборудование неактивно**, чтобы SNMP-агент не отправлял SNMP-менеджеру уведомление-ловушку, когда компонент, на котором установлен SNMP-агент, переходит в неактивное состояние.

   По умолчанию флажки установлены.

10. Нажмите на кнопку **Назад**, чтобы продолжить указывать параметры уведомления-ловушки.
11. В поле **Описание** введите краткое описание уведомления-ловушки.
12. Нажмите на кнопку **Сохранить**.

Уведомление-ловушка будет создано и отобразится в таблице.

Изменение уведомления-ловушки

Чтобы изменить уведомление-ловушку:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, к которому подключены компоненты для мониторинга.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **SNMP**.

   Отобразится таблица уведомлений-ловушек.

4. В блоке **Параметры ловушки** нажмите на кнопку **Изменить**.
5. В открывшемся окне при необходимости измените параметры уведомления-ловушки. Описание параметров см. в инструкции по созданию уведомления-ловушки.
6. Нажмите на кнопку **Сохранить**.

Уведомление-ловушка будет изменено и обновится в таблице.

Удаление уведомления-ловушки

Удаленные уведомления-ловушки невозможно восстановить.

Чтобы удалить уведомление-ловушку:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, к которому подключены компоненты для мониторинга.

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **SNMP**.

   Отобразится таблица уведомлений-ловушек.

4. В блоке **Параметры ловушки** нажмите на кнопку **Изменить**.

5. В открывшемся окне нажмите на кнопку **Удалить** рядом с уведомлением-ловушкой, которое вы хотите удалить.

6. Нажмите на кнопку **Сохранить**.

Уведомление-ловушка будет удалено и перестанет отображаться в таблице.

Мониторинг соединения

Чтобы включить мониторинг соединения:

1. Перейдите ко включению мониторинга соединения одним из следующих способов:

   - Если вы хотите включить мониторинг соединения, установленного с устройства CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Соединения** и нажмите на кнопку **Управление** → **Установить пороговые значения** рядом с соединением.

   - Если вы хотите включить мониторинг одного из соединений в таблице всех соединений, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Соединения** и нажмите на кнопку **Управление** → **Установить пороговые значения** рядом с соединением.

   - Если вы хотите включить мониторинг одного из соединений в графической топологии со всеми соединениями, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Топология**, нажмите на соединение и нажмите на кнопку **Установить пороговые значения**.

2. Установите флажок **Включить мониторинг пороговых значений**, чтобы включить мониторинг соединения. Этот флажок снят по умолчанию.

3. Если вы хотите указать пороговые значения показателей мониторинга соединения, выполните следующие действия:

   a. Если вы хотите установить пороговые значения показателей мониторинга соединения по умолчанию, нажмите на кнопку **Параметры по умолчанию**.

   b. Если вы хотите, чтобы контроллер использовал соединение в последнюю очередь при расчете пути независимо от показателей мониторинга, установите флажок **Последний вариант**. Этот флажок снят по умолчанию.

   c. В поле **Интервал обработки ошибок и степени использования (сек.)** введите интервал времени в секундах для измерения количества ошибок на соединении и уровня его загруженности. Диапазон значений: от 1 до 300. Значение по умолчанию: `60`.

   d. Если вы хотите указать пороговое значение количества ошибок в секунду на соединении, установите флажок **Включить мониторинг ошибок** и в поле **Уровень критических ошибок (ошибок/сек.)** введите пороговое значение. Диапазон значений: от 1 до 1 000 000. Этот флажок снят по умолчанию, и в поле введено значение `1000`.

   e. Если вы хотите указать пороговое значение загруженности соединения в процентах от скорости сервисного интерфейса источника, установите флажок **Включить мониторинг использования** и в поле **Критический уровень использования (%)** введите пороговое значение. Этот флажок снят по умолчанию, и в поле введено значение `95`.

   f. В поле **Интервал обработки задержки, джиттера и потери пакетов (сек.)** введите интервал времени в секундах для измерения показателей задержки, джиттера и потерь пакетов на соединении. Диапазон значений: от 1 до 600. Значение по умолчанию: `30`.

   g. Если вы хотите указать пороговое значение времени задержки в миллисекундах при передаче трафика через соединение, установите флажок **Включить мониторинг задержек** и в поле **Критический уровень задержек (мс)** введите пороговое значение. Диапазон значений: от 5 до 1000. Этот флажок снят по умолчанию, и в поле введено значение `100`.

   h. Если вы хотите указать пороговое значение времени джиттера в миллисекундах при передаче трафика через соединение, установите флажок **Включить мониторинг джиттера** и в поле **Критический уровень джиттера (мс)** введите пороговое значение. Диапазон значений: от 5 до 1000. Этот флажок снят по умолчанию, и в поле введено значение `100`.

   i. Если вы хотите указать пороговое значение процента потерь пакетов трафика на соединении, установите флажок **Включить мониторинг потерь пакетов** и в поле **Критический уровень потерь пакетов (%)** введите пороговое значение. Диапазон значений: от 1 до 100. Этот флажок снят по умолчанию, и в поле введено значение `2`.

   Указанные пороговые значения показателей мониторинга будут использоваться пороговыми ограничениями.

4. Сохраните параметры мониторинга соединения одним из следующих способов:

   - Если вы хотите сохранить параметры мониторинга соединения, нажмите на кнопку **Сохранить**.

   - Если вы хотите сохранить параметры мониторинга соединения и указать такие же параметры на встречном соединении, нажмите на кнопку **Сохранить для обоих соединений**.

5. Если вы указали параметры мониторинга соединения, установленного с устройства CPE, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Построение сети SD-WAN между устройствами CPE

Для передачи трафика вам нужно построить сеть SD-WAN между устройствами CPE с помощью соединений (англ. links), которые строятся поверх нижележащей сети. Устройства CPE строят соединения со всех доступных интерфейсов SD-WAN с типом WAN. Соединения являются однонаправленными. Это значит, что при построении соединения от устройства CPE 1 до устройства CPE 2 автоматически строится соединение от устройства CPE 2 до устройства CPE 1. Перед построением сети SD-WAN требуется обеспечить сетевую связность между устройствами CPE.

Соединения строятся на основании ролей, которые вы назначаете устройствам CPE. Вы можете назначить устройству CPE роль шлюза SD-WAN или стандартного устройства CPE. Шлюзы SD-WAN строят соединения со всеми стандартными устройствами CPE и другими шлюзами SD-WAN. Стандартные устройства CPE строят соединения только со шлюзами SD-WAN. По умолчанию всем устройствам CPE назначена роль стандартных устройств CPE.

Если вы хотите, чтобы между двумя стандартными устройствами CPE было построено соединение, вам нужно назначить им одинаковый топологический тег. Вы можете сделать стандартное устройство CPE транзитным, чтобы другие устройства CPE могли строить через него соединения.

Соединения между устройствами CPE образуют топологию. В Kaspersky SD-WAN наиболее распространены следующие топологии:

- Hub-and-Spoke – соединения между устройствами CPE строятся через шлюзы SD-WAN.
- Full-Mesh и Partial-Mesh – соединения между устройствами CPE строятся напрямую, либо частично напрямую, частично через шлюзы SD-WAN.

В рамках сети SD-WAN трафик между устройствами CPE может передаваться по нескольким путям. Пути проходят через соединения между устройствами CPE. Совокупность всех возможных путей между двумя устройствами CPE называется *сегментом*. Трафик может быть разделен по нескольким путям на устройстве CPE источника сегмента и передан устройству CPE назначения сегмента. Один сегмент может содержать от 2 до 16 путей.

Поддерживаются следующие типы путей:

- *Auto-SPF* (Shortest-Path Forwarding) – автоматически рассчитываемый контроллером путь. Вы можете передавать трафик по путям Auto-SPF в двух режимах:

  - *Active/Active* – при передаче трафика между устройствами CPE одновременно используются несколько путей Auto-SPF.

  - *Active/Standby* – при передаче трафика между устройствами CPE используется один путь Auto-SPF с наименьшей стоимостью. Если используемый путь Auto-SPF становится недоступным, используется следующий путь Auto-SPF с наименьшей стоимостью. Стоимость пути складывается из стоимости каждого соединения, через которые проходит путь. Вы можете указать стоимость соединений вручную.

  Вы можете определить режим передачи трафика по путям Auto-SPF при настройке путей.

- *Auto-TE* (Traffic Engineering) – автоматически рассчитываемый контроллером путь, учитывающий указанные вами пороговые ограничения.

- *Manual-TE* – путь, который вы создаете вручную. При создании пути Manual-TE вам нужно указать соединения, через которые путь проходит от устройства CPE источника сегмента до устройства CPE назначения сегмента.

О топологии Hub-and-Spoke

В рамках топологии Hub-and-Spoke центральная площадка (англ. hub site) подключается к нескольким удаленным площадкам (англ. spoke sites) для обмена трафиком. Эта топология является наиболее распространенной при построении сетей SD-WAN, так как упрощает процесс управления сетью и предоставляет более высокий уровень безопасности путем маршрутизации трафика через центральную площадку, где выполняется анализ и типизация трафика. Использование топологии Hub-and-Spoke также позволяет более эффективно использовать полосу пропускания за счет оптимизации и приоритизации трафика на центральной площадке.

Для построения топологии Hub-and-Spoke вам нужно назначить устройствам CPE роли шлюзов SD-WAN и стандартных устройств CPE. В этом случае шлюзы SD-WAN строят соединения с другими шлюзами SD-WAN и стандартными устройствами CPE, а стандартные устройства CPE строят соединения только со шлюзами SD-WAN.

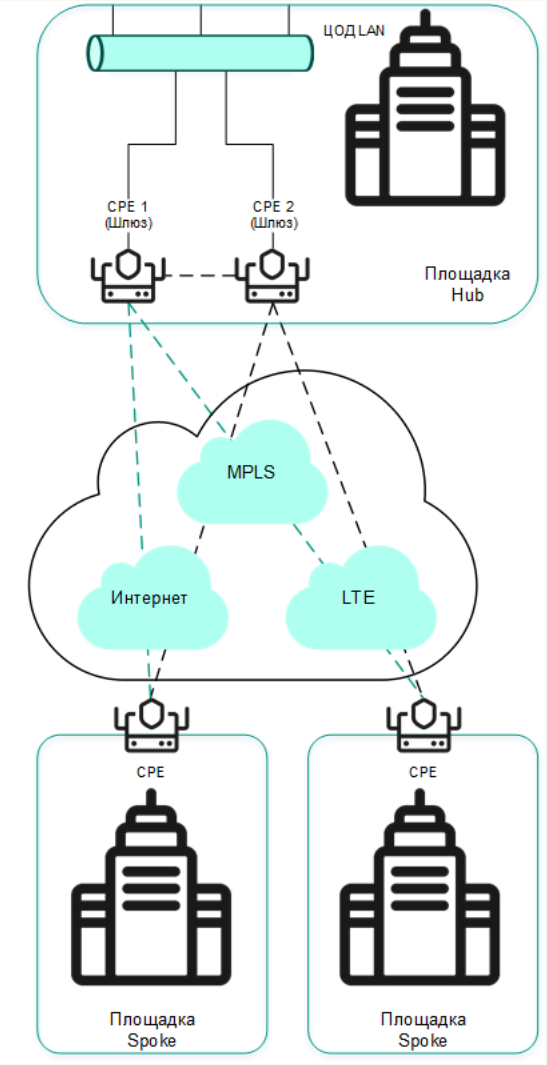
Вы можете использовать качество обслуживания, чтобы ограничить полосу пропускания для устройств CPE или классов трафика.

Примеры топологии Hub-and-Spoke:

- Топология Hub-and-Spoke без связи между удаленными площадками.

  На рисунке ниже представлена топология Hub-and-Spoke, в рамках которой удаленные площадки связываются с центральной площадкой и не могут напрямую связаться друг с другом. Сети SD-WAN, построенные с применением этой топологии, просты в проектировании и обслуживании, потому что все необходимые сетевые сервисы и приложения размещаются в одном центре обработки данных.

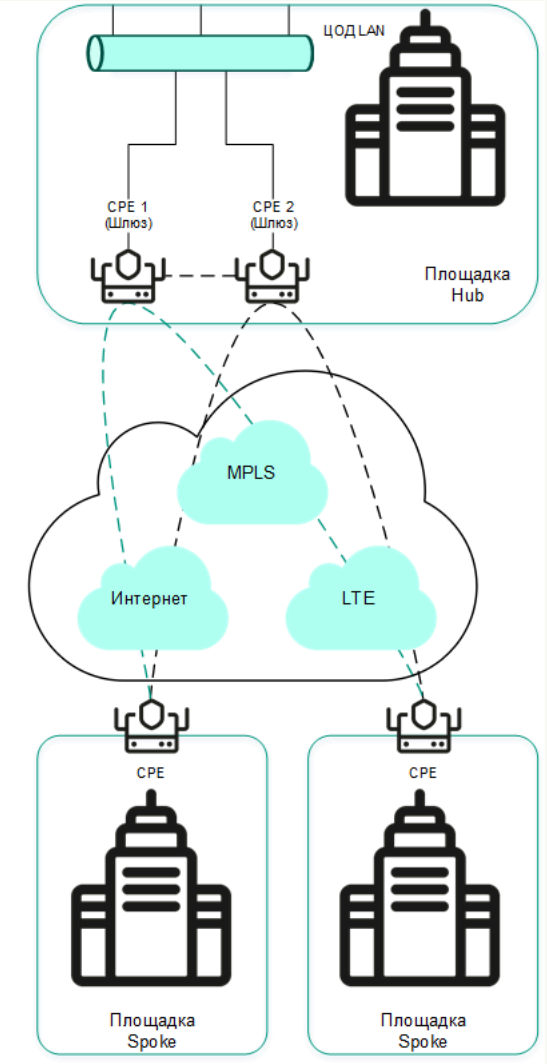
  При регистрации устройства CPE автоматически добавляются в управляющий транспортный сервис с ролью Leaf и могут находиться за NAT (Network Address Translation) и PAT (Port Address Translation). В рамках такой топологии Hub-and-Spoke невозможна передача трафика напрямую между устройствами CPE.



Топология Hub-and-Spoke без связи между удаленными площадками

- Топология Hub-and-Spoke со связью между удаленными площадками через центральную площадку.

На рисунке ниже представлена топология Hub-and-Spoke, в рамках которой удаленные площадки могут связываться друг с другом через центральную площадку. При регистрации устройства CPE автоматически добавляются в управляющий транспортный сервис и могут находиться за NAT и PAT.



Топология Hub-and-Spoke со связью между удаленными площадками через центральную площадку

О топологиях Full-Mesh и Partial-Mesh

В рамках топологий Full-Mesh и Partial-Mesh между стандартными устройствами CPE строятся соединения. Построение соединений между стандартными устройствами CPE имеет следующие преимущества по сравнению с топологией Hub-and-Spoke, в рамках которой стандартные устройства CPE связываются друг с другом через шлюзы SD-WAN:

- Улучшенные характеристики качества соединений, такие как задержка (англ. delay), потеря пакетов (англ. loss) и джиттер (англ. jitter).
- Большая пропускная способность соединений.
- Сохранение аппаратных ресурсов шлюзов SD-WAN.

Для построения топологии Full-Mesh вам нужно назначить устройствам CPE роль стандартных устройств CPE и назначить стандартным устройствам CPE один и тот же топологический тег. В этом случае стандартные устройства CPE с одинаковыми топологическими тегами строят соединения друг с другом.

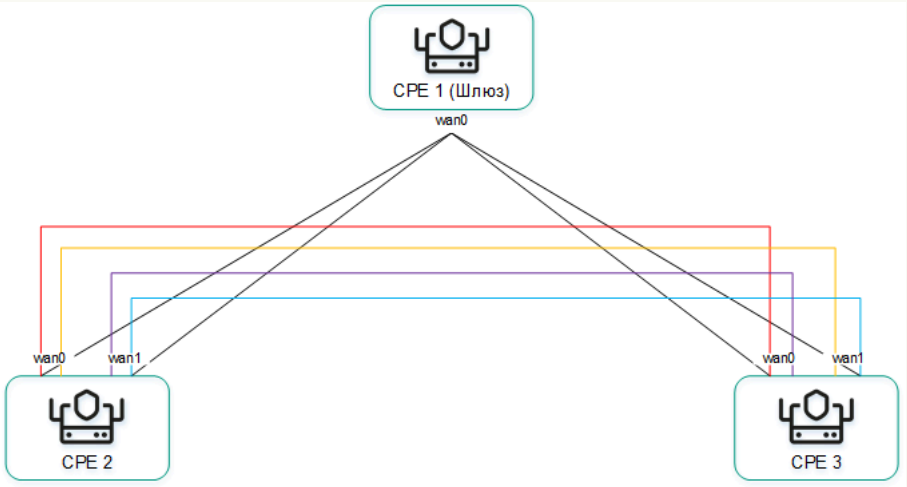
Для построения топологии Partial-Mesh вам нужно назначить устройствам CPE роли шлюзов SD-WAN и стандартных устройств CPE, а также назначить стандартным устройствам CPE один и тот же топологический тег. В этом случае шлюзы SD-WAN строят соединения с другими шлюзами SD-WAN и стандартными устройствами CPE, а стандартные устройства CPE строят соединения со шлюзами SD-WAN и друг с другом, если стандартным устройствам CPE назначен одинаковый топологический тег. Если вы хотите разделить стандартные устройства CPE на группы, вам нужно назначить стандартным устройствам CPE в каждой группе уникальный топологический тег, а также назначить хотя бы одному стандартному устройству CPE в каждой группе одинаковый топологический тег.

Вы можете использовать качество обслуживания, чтобы ограничить полосу пропускания для устройств CPE или классов трафика.

Примеры топологий Full-Mesh и Partial-Mesh:

- **Топология Full-Mesh**

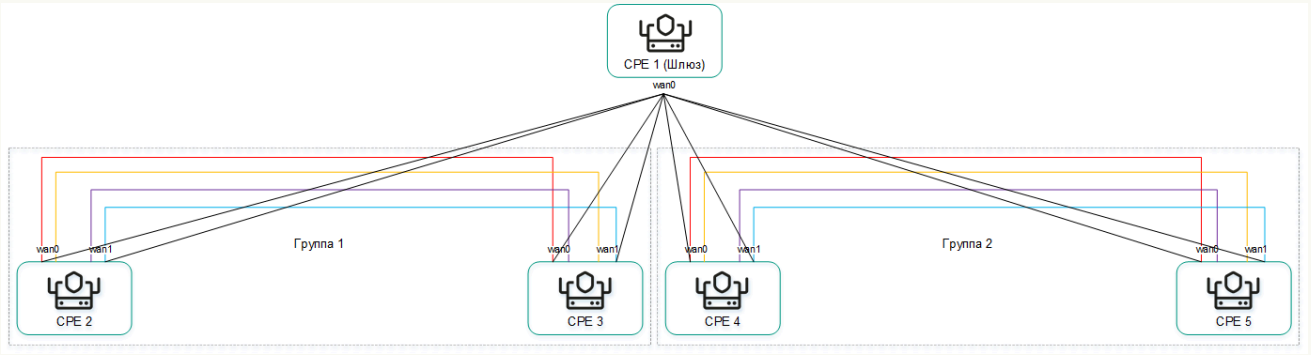
  На рисунке ниже представлена топология Full-Mesh, в рамках которой все устройства CPE строят соединения друг с другом. Трафик между устройствами CPE 2 и CPE 3 пересылается напрямую. При большом количестве устройств CPE и соединений такая топология может оказаться чрезвычайно требовательной к ресурсам контроллера.

  Топология Full-Mesh

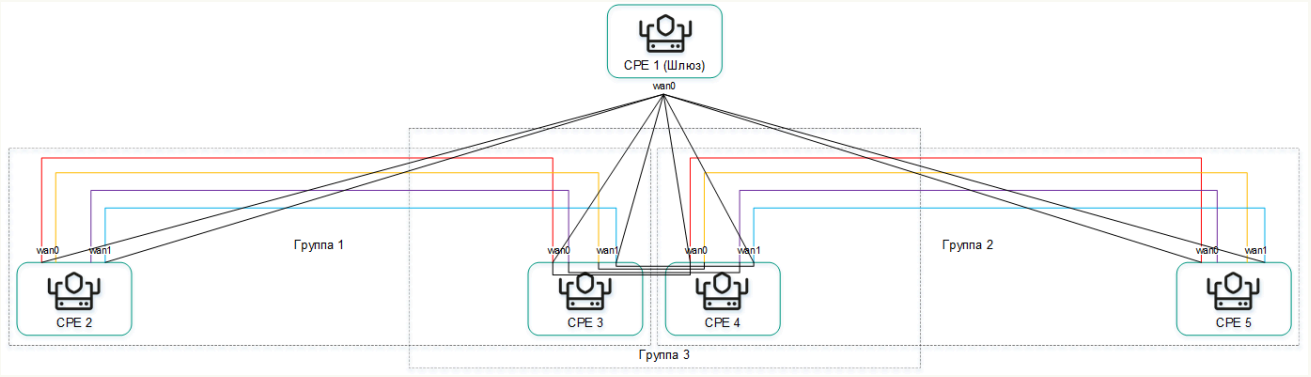
- **Топология Partial-Mesh**

На рисунке ниже представлена топология Partial-Mesh. Такая топология используется, когда соединения между некоторыми устройствами CPE могут быть нежелательны по административным причинам или невозможны по техническим причинам. В этой топологии вы можете сгруппировать устройства CPE таким образом, что устройства CPE в одной группе связываются друг с другом напрямую и связываются с устройствами CPE из других групп через транзитное устройство CPE.



Топология Partial-Mesh

Устройство CPE может входить одновременно в несколько групп, как показано на рисунке ниже.

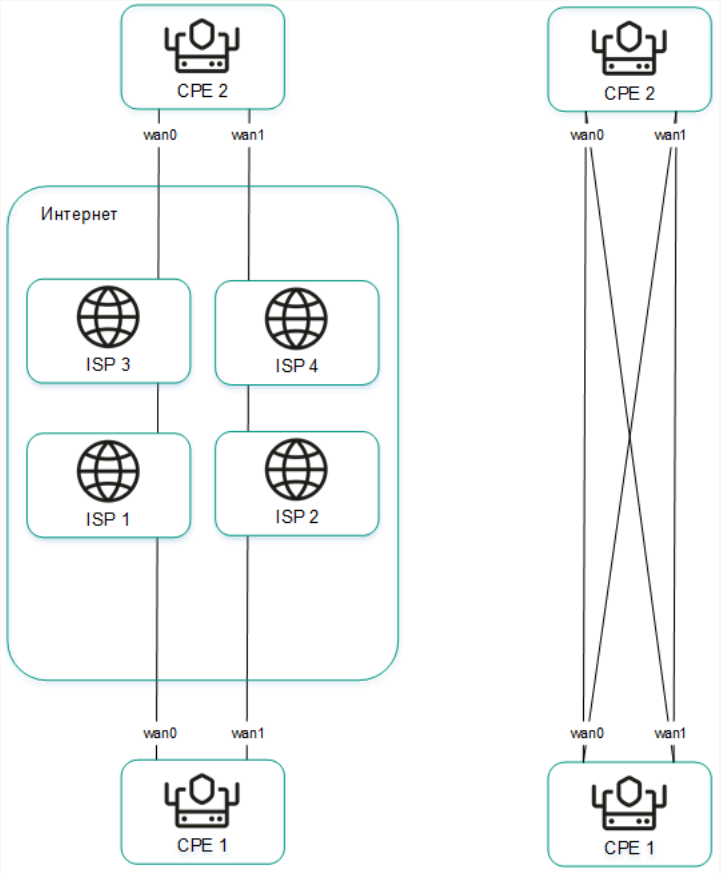


Топология Partial-Mesh, устройства CPE входят в несколько групп

При построении соединений между устройствами CPE, в зависимости от типа связности устройств CPE через физические соединения, возможны следующие варианты наложенной связности:

- **Все физические соединения имеют прямую IP-связность между собой**.

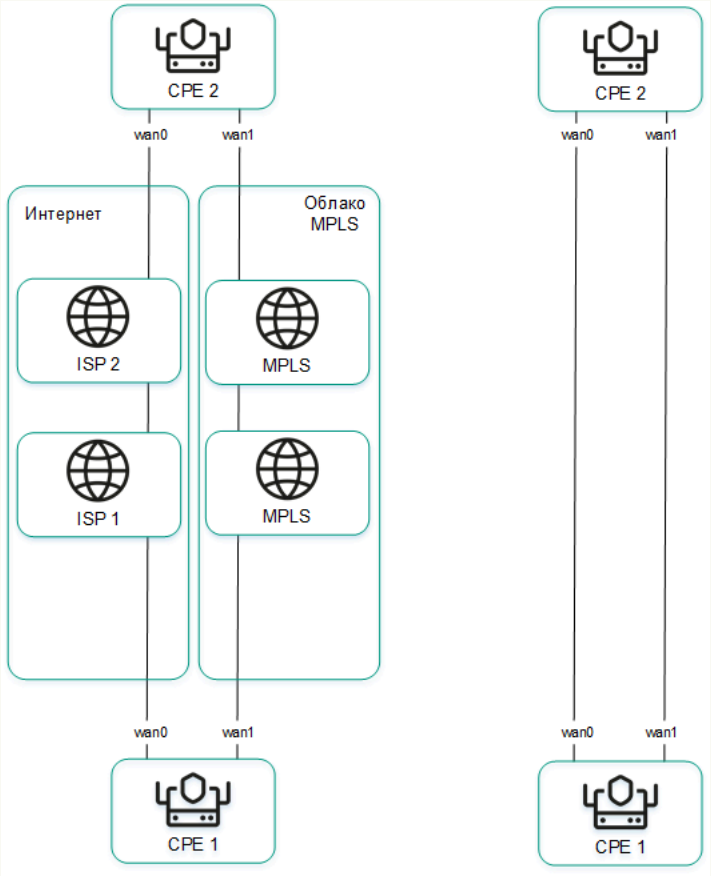
  За счет связности в пределах интернета устройства CPE могут построить максимальное количество соединений между собой (см. рисунок ниже).

  Полная физическая связность между устройствами CPE

- **Физические соединения имеют частичную IP-связность между собой**.

На рисунке ниже облако интернета и облако MPLS не связаны между собой, поэтому соединения можно построить только через интерфейсы SD-WAN с типом WAN, принадлежащие одному и тому же облаку. Соединения CPE1:WAN0 → CPE2:WAN1 и CPE1:WAN1 → CPE2:WAN0 невозможно построить.



Возможны и другие сценарии связности наложенной сети, если IP-связность между SD-WAN интерфейсами с типом WAN устройств CPE в пределах одного облака невозможна по другим причинам, например при использовании топологии MPLS, не поддерживающей прямую связь между устройствами CPE, либо из-за наличия NAT/PAT или ACL в интернете.

Назначение роли устройству CPE

Вы можете назначить роль шаблону CPE или устройству CPE. Роль, назначенная шаблону CPE, автоматически назначается всем устройствам CPE, которые используют шаблон CPE.

Чтобы назначить роль устройству CPE:

1. Перейдите к назначению роли устройству CPE одним из следующих способов:

   - Если вы хотите назначить роль шаблону CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Топология**.
   - Если вы хотите назначить роль устройству CPE, выполните одно из следующих действий:
     - В меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Топология** и установите флажок **Переопределить**.
     - В меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, перейдите в раздел **Топологические теги** и в раскрывающемся списке **Коммутатор** выберите устройство CPE.

2. В раскрывающемся списке **Роль** выберите роль устройства CPE:

   - **CPE** – стандартное устройство CPE. Это значение выбрано по умолчанию.
   - **Шлюз** – шлюз SD-WAN. Вы не можете назначать топологические теги шлюзам SD-WAN.

3. Сохраните роль устройства CPE одним из следующих способов:

   - Если вы назначили роль шаблону CPE или устройству CPE в разделе **SD-WAN**, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE.
   - Если вы назначили роль устройству CPE в разделе **Топологические теги**, нажмите на кнопку **Сохранить**.

Роль будет назначена устройству CPE.

Назначение топологического тега устройству CPE

Вы можете назначить топологический тег шаблону CPE или устройству CPE. Топологический тег, назначенный шаблону CPE, автоматически назначается всем устройствам CPE, которые используют шаблон CPE. Устройства CPE с одинаковыми топологическими тегами автоматически строят соединения друг с другом. Топологический тег невозможно назначить устройству CPE, если вы назначили устройству CPE роль шлюза SD-WAN.

Чтобы назначить топологический тег устройству CPE:

1. Перейдите к назначению топологического тега устройству CPE одним из следующих способов:

   - Если вы хотите назначить топологический тег шаблону CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Топология**.

   - Если вы хотите назначить топологический тег устройству CPE, выполните одно из следующих действий:

     - В меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Топология** и установите флажок **Переопределить**.

     - В меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Топологические теги** и в раскрывающемся списке **Коммутатор** выберите устройство CPE.

   Отобразятся топологические теги.

2. В поле **Топологические теги** введите топологический тег, который вы хотите назначить устройству CPE, и нажмите на значок добавления +.

   Топологический тег будет назначен устройству CPE. Вы можете назначить несколько топологических тегов и удалить топологический тег. Для удаления топологического тега нажмите рядом с ним на значок удаления ×.

3. Сохраните топологические теги устройства CPE одним из следующих способов:

   - Если вы назначили топологический тег шаблону CPE или устройству CPE в разделе **SD-WAN**, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE.

   - Если вы назначили топологический тег устройству CPE в разделе **Топологические теги**, нажмите на кнопку **Сохранить**.

Настройка путей

Вы можете настроить пути в сегменте, шаблоне CPE или на устройстве CPE. Параметры путей, указанные в сегменте или шаблоне CPE, автоматически распространяются на все устройства CPE, которые входят в сегмент или используют шаблон CPE. Параметры путей, указанные на устройстве CPE, автоматически распространяются на все устройства CPE, которые входят в один сегмент с устройством CPE.

Чтобы настроить пути:

1. Перейдите к настройке путей одним из следующих способов:

   - Если вы хотите настроить пути в сегменте, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Сегменты** и нажмите на кнопку **Управление** → **Изменить** рядом с сегментом.

   - Если вы хотите настроить пути в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Мультипутевая передача**.

   - Если вы хотите настроить пути на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE и выберите вкладку **Мультипутевая передача**.

   Отобразятся параметры путей.

2. В поле **Максимум транспортных путей** введите максимальное количество путей, поддерживаемое устройством CPE или сегментом. Диапазон значений: от 1 до 16. Значение по умолчанию: `8`.

3. В поле **Максимум Auto-SPF** введите максимальное количество путей Auto-SPF, поддерживаемое устройством CPE или сегментом. Пути Auto SPF автоматически рассчитываются контроллером. Диапазон значений: от 1 до 8. Значение по умолчанию: `2`.

   Если вы хотите, чтобы трафик передавался между устройствами CPE в режиме Active/Active, введите значение больше `1` в этом поле. Если вы хотите, чтобы трафик передавался между устройствами CPE в режиме Active/Standby, введите значение `1` в этом поле.

4. В поле **Множитель разброса стоимости** введите во сколько раз стоимость пути может быть больше стоимости пути с самой низкой стоимостью в вашей сети SD-WAN, чтобы этот путь был добавлен в сегмент. Диапазон значений: от 1.0 до 10.0. Значение по умолчанию: `10`. Вы не можете ввести значение в этом поле, если установлен флажок **Балансировка трафика с учетом веса**.

   Например, если вы ввели `2` в этом поле и наименьшая стоимость пути в вашей сети SD-WAN составляет 10 000, в сегмент могут быть добавлены пути со стоимостью до 20 000. В режиме Active/Standby значение в этом поле определяет, какой путь Auto-SPF используется, если предыдущий путь Auto-SPF становится недоступным.

5. Если вы хотите, чтобы пути добавлялись в сегмент вне зависимости от их стоимости, установите флажок **Балансировка трафика с учетом веса**. Этот флажок снят по умолчанию.

6. Если вы настраиваете пути в сегменте, при необходимости добавьте или измените пути Manual TE.

7. Сохраните параметры путей одним из следующих способов:

   - Если вы настроили пути в сегменте, нажмите на кнопку **Сохранить**, чтобы сохранить параметры сегмента.

   - Если вы настроили пути в шаблоне CPE или на устройстве CPE:

     В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE немедленно, или запланируйте отложенное сохранение, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

   Параметры путей будут сохранены.

Работа с соединениями

Вы можете посмотреть соединения одним из следующих способов:

- Для просмотра таблицы соединений, установленных с устройства CPE, вам нужно в меню перейти в раздел **SD-WAN → CPE**, нажать на устройство CPE и выбрать вкладку **Соединения**.
- Для просмотра таблицы всех соединений вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление → Параметры развертывания** рядом с контроллером и перейти в раздел **Соединения**.
- Для просмотра графической топологии со всеми соединениями вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление → Параметры развертывания** рядом с контроллером и перейдите в раздел **Топология**.

При просмотре таблицы соединений информация о соединениях отображается в следующих столбцах таблицы:

- **Источник** – имя, идентификатор DPID и номер OpenFlow-порта устройства CPE источника соединения.
- **IP/порт источника** – IP-адрес и номер порта источника соединения, разделенные двоеточием.
- **NAT/Изоляция ист** – топологический признак источника соединения, отвечающий за передачу контроллеру информации об интерфейсах SD-WAN. Возможные значения:
  - **N** (Выключено. Информация об интерфейсе SD-WAN не передается контроллеру).
  - **NAT/PAT** (интерфейс SD-WAN находится за NAT или PAT).
  - **Изолированная WAN** (интерфейс SD-WAN подключен к изолированной сети).
- **Назначение** – имя, идентификатор DPID и номер OpenFlow-порта устройства CPE назначения соединения.
- **IP/порт назначения** – IP-адрес и номер порта назначения соединения, разделенные двоеточием.
- **NAT/Изоляция наз** – топологический признак назначения соединения, отвечающий за передачу контроллеру информации об интерфейсах SD-WAN. Возможные значения:
  - **N** (Выключено. Информация об интерфейсе SD-WAN не передается контроллеру).
  - **NAT/PAT** (интерфейс SD-WAN находится за NAT или PAT).
  - **Изолированная WAN** (интерфейс SD-WAN подключен к изолированной сети).

  При необходимости вы можете скрыть все столбцы, кроме **Источник**, **IP/порт источника**, **NAT/Изоляция ист**, **Назначение**, **IP/порт назначения**, **NAT/Изоляция наз**, нажав на значок настройки и выбрав в меню пункт **Показать IP туннелей**.

- **Последний вариант** – контроллер использует соединение в последнюю очередь при расчете пути независимо от показателей мониторинга:
  - **Y**.
  - **N**.
- **Пороговый мониторинг** – использование порогового мониторинга соединения. Возможные значения:
  - **Y** (мониторинг включен).
  - **N** (мониторинг включен).
- **Шифрование** – статус шифрования соединения. Возможные значения:
  - **Настроено**
  - **Включено**
  - **Выключено**
- **CFM –** интервал времени для отправки контрольных пакетов при работе функции Connectivity Fault Management. В этом столбце отображаются два значения в формате **<значение 1>/<значение 2>**:
  - **<значение 1>** – это интервал времени для отправки контрольных пакетов, который вы указали при включении функции CFM на устройстве CPE.
  - **<значение 2>** – используемый интервал времени для отправки контрольных пакетов. Для отправки контрольных пакетов может использоваться один из следующих интервалов времени:
    - Интервал времени для отправки контрольных пакетов, который вы указали при включении функции CFM на устройстве CPE. Если вы указываете на устройствах CPE разные интервалы времени для отправки контрольных пакетов, используется самый большой из указанных интервалов времени. Например, если на устройстве CPE 1 в качестве интервала времени для отправки контрольных пакетов указано 300 миллисекунд, а на устройстве CPE 2 указана одна секунда, интервалом времени для отправки контрольных пакетов будет одна секунда.
    - Интервал времени для отправки контрольных пакетов, который вы указали при включении функции CFM на соединении. Интервал времени для отправки контрольных пакетов на соединении имеет приоритет перед интервалами времени для отправки контрольных пакетов на устройствах CPE. Например, если на устройстве CPE 1 в качестве интервала времени для отправки контрольных пакетов указано 300 миллисекунд, на устройстве CPE 2 указана одна секунда, а на соединении между устройствами CPE 1 и 2 указано 10 секунд, интервалом времени для отправки контрольных пакетов будет 10 секунд.

  Если одно из значений в столбце подчеркнуто, это значит, что вы указали значение вручную.
- **MTU** – значение MTU на соединении.
- **Ошибок/секунду** – количество ошибок в секунду на соединении.
- **Использование (%)** – загруженность соединения в процентах от скорости сервисного интерфейса источника.
- **Задержка (мс)** – время задержки в миллисекундах при передаче трафика через соединение.

- **Джиттер (мс)** – время джиттера в миллисекундах при передаче трафика через соединение.
- **Потеря пакетов (%)** – процент потерь пакетов трафика на соединении.
- **Скорость (Мбит/сек.)** – скорость передачи трафика через соединение в мегабитах в секунду.
- **Состояние конфигурации FEC / Операционное состояние FEC** – статус конфигурации / работы функции Forward Error Correction на соединении (**Включено** или **Выключено**).
- **Стоимость** – стоимость соединения.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Просмотр статистики соединения

Чтобы посмотреть статистику соединения:

1. Перейдите к просмотру статистики соединения одним из следующих способов:

   - Если вы хотите просмотреть статистику соединения, установленного с устройства CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, в разделе **Соединения** нажмите на кнопку **Управление** для нужного соединения и выберите **Просмотреть статистику**.

   - Если вы хотите просмотреть статистику одного из соединений в таблице всех соединений, в меню перейдите в раздел **Инфраструктура**, рядом с контроллером нажмите на кнопку **Управление** и выберите **Параметры развертывания**, затем в разделе **Соединения** нажмите на кнопку **Управление** для нужного соединения и выберите **Просмотреть статистику**.

   - Если вы хотите просмотреть статистику одного из соединений в графической топологии со всеми соединениями, в меню перейдите в раздел **Инфраструктура**, рядом с контроллером нажмите на кнопку **Управление** и выберите **Параметры развертывания**, затем в разделе **Топология** нажмите на соединение и выберите **Просмотреть статистику**.

   Откроется окно со статистикой соединения. Статистика разбита на таблицы, расположенные на соответствующих вкладках: **Данные телеметрии**, **Шифрование**, CFM, FEC.

   Эффективная конфигурация

   Источник конфигурации

   Коммутатор

   Тип

   Включено

   Интервал

   1s

   Операционное состояние

   Тип

   Включено

   Интервал

   1s

   FEC

   Эффективная конфигурация

   Источник конфигурации

   Коммутатор

   Тип

   Выключено

   Степень избыточности

   Максимальное время в буфере реорганизации (мс)

   Операционное состояние

   Тип

   Выключено

Степень избыточности

Максимальное время в буфере реорганизации (мс)

Послано оригинальных пакетов

Послано пакетов FEC

Степень избыточности в пакетах (%)

Послано оригинальных байт

Послано байт FEC

Степень избыточности в байтах (%)

Скорость передачи оригинальных пакетов (пакет/сек.)

Полная скорость передачи пакетов (пакет/сек.)

Скорость передачи оригинальных данных (Кбит/сек.)

Полная скорость передачи данных (Кбит/с)

Доля потерянных оригинальных пакетов (%)

Общая доля потерянных пакетов (%)

Автоматическое изменение стоимости соединения в зависимости от максимальной скорости интерфейса

Если скорость WAN-интерфейса SD-WAN на устройстве CPE выше скорости сети, предоставляемой оператором связи, вам нужно ограничить максимальную скорость (англ. Maximum rate) этого интерфейса в соответствии со скоростью сети.

Пример:
Оператор связи предоставляет клиенту доступ в интернет на скорости 50 мегабит, а скорость физического подключения на интерфейсе устройства CPE составляет 100 мегабит. В этом случае для правильного расчета стоимости на соединениях и QoS необходимо указать значение максимальной скорости равным 50.

Вы можете указать максимальную скорость при создании или изменении исходящего интерфейса SD-WAN, участвующего в соединении. На основе наименьшего значения максимальной скорости обоих интерфейсов на концах соединения вычисляется значение стоимости (англ. cost) соединения. Параметры максимальной скорости и стоимости связаны следующим образом:

- Максимальная скорость задает максимальную пропускную способность интерфейса для правильного расчета логических очередей для QoS. Измеряется в Мбит/с.

- Стоимость определяет вес интерфейса в топологии и рассчитывается по формуле `Cost = 10 000 000 / Speed`, где `Speed` равно значению максимальной скорости. Чем меньше значение стоимости, тем более приоритетным является соединение в топологии сети.

При изменении максимальной скорости значение стоимости меняется для соединений в обоих направлениях. Для соединения берется наименьшее значение максимальной скорости участвующих в нем интерфейсов.

Помимо автоматического вычисления стоимости соединения, вы можете указать его стоимость вручную.

Указание стоимости соединения

Чтобы указать стоимость соединения:

1. Перейдите к указанию стоимости соединения одним из следующих способов:

   - Если вы хотите указать стоимость соединения, установленного с устройства CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Соединения** и нажмите на кнопку **Управление** → **Указать стоимость** рядом с соединением.

   - Если вы хотите указать стоимость одного из соединений в таблице всех соединений, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Соединения** и нажмите на кнопку **Управление** → **Указать стоимость** рядом с соединением.

   - Если вы хотите указать стоимость одного из соединений в графической топологии со всеми соединениями, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Топология**, нажмите на соединение и нажмите на кнопку **Указать стоимость**.

2. В открывшемся окне установите флажок **Переопределить**, чтобы указать стоимость соединения. Этот флажок снят по умолчанию.

3. В поле **Стоимость соединения** введите стоимость соединения. Если вы хотите указать такую же стоимость для встречного соединения, установите флажок **Сохранить для обоих соединений**. Этот флажок снят по умолчанию.

4. Нажмите на кнопку **Сохранить**.

   Стоимость соединения будет указана.

5. Если вы указали стоимость соединения, установленного с устройства CPE, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Включение функции Dampening

Функция *Dampening* – это настраиваемый механизм, исключающий использование нестабильных соединений, состояние которых меняется слишком часто, при расчете путей. Для определения нестабильности соединений учитываются изменения следующих состояний:

- UP/LIVE → DOWN/NOT-LIVE.
- DOWN/NOT-LIVE → UP/LIVE.
- UP/LIVE → UP/NOT-LIVE.
- UP/NOT-LIVE → UP/LIVE.

Когда функция Dampening включена на соединении, каждое изменение состояния соединения, увеличивает значение показателя Penalty. Если показатель Penalty достигает порогового значения за указанный промежуток времени, доступ к соединению ограничивается (его стоимость повышается в 10 000 раз на указанный промежуток времени). Вы указываете значение каждого из этих параметров при включении функции Dampening. По умолчанию доступ к соединению возобновляется, если в течение 10 минут не происходит ни одного изменения состояния соединения.

Чтобы включить функцию Dampening:

1. Перейдите ко включению функции Dampening одним из следующих способов:

   - Если вы хотите включить функцию Dampening на соединении, установленном с устройства CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Соединения** и нажмите на кнопку **Управление → Dampening** рядом с соединением.

   - Если вы хотите включить функцию Dampening на одном из соединений в таблице всех соединений, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, перейдите в раздел **Соединения** и нажмите на кнопку **Управление → Dampening** рядом с соединением.

   - Если вы хотите включить функцию Dampening на одном из соединений в графической топологии со всеми соединениями, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, перейдите в раздел **Топология**, нажмите на соединение и нажмите на кнопку **Dampening**.

2. В открывшемся окне установите флажок **Включить**, чтобы включить функцию Dampening на соединении. Этот флажок снят по умолчанию.

3. В поле **Максимальное время блокировки (мс)** введите время в миллисекундах, в течение которого доступ к соединению может быть ограничен. По истечении указанного времени все счетчики функции Dampening на соединении сбрасываются. Значение по умолчанию: `600000`.

4. В поле **Штраф** введите число, которое прибавляется к показателю Penalty при изменении состояния соединения. Значение по умолчанию: `1`.

5. В поле **Порог блокировки** введите значение показателя Penalty, при котором доступ к соединению ограничивается. Значение по умолчанию: `4`.

6. В поле **Интервал обновления (мс)** введите время в миллисекундах, за которое показатель Penalty должен набрать значение, указанное в поле **Порог блокировки**, чтобы доступ к соединению был ограничен. Значение по умолчанию: `120000`.

7. Если вы хотите посмотреть статистику работы функции Dampening на соединении, нажмите на кнопку **Загрузить статистику**.

8. Нажмите на кнопку **Сохранить**.

   Функция Dampening будет включена на соединении.

9. Если вы включили функцию Dampening на соединении, установленном с устройства CPE, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Включение функции Forward Error Correction

Функция *Forward Error Correction* или *прямая коррекция ошибок* (далее также FEC) снижает потери пакетов трафика на соединениях, особенно для UDP-приложений, и количество повторных передач пакетов (англ. retransmissions), которые ведут к задержкам, а также восстанавливает принимаемые данные на устройстве CPE. Восстановление данных обеспечивается избыточным кодированием потока данных на устройстве CPE источника.

Когда функция FEC включена на соединении, устройство CPE источника кодирует поток передающихся через соединение пакетов трафика и добавляет избыточные пакеты трафика. Использование кодирования на устройствах CPE может привести к задержкам, вызванным дополнительной обработкой данных.

Устройство CPE назначения буферизует принятые через соединение пакеты трафика и декодирует их, восстанавливая потерянные пакеты трафика, если это возможно. Мы рекомендуем использовать FEC на noisy links (или зашумленных соединениях) для уменьшения потери пакетов трафика и увеличения скорости TCP-соединений. Общая схема работы функции FEC представлена на рисунке ниже.



Схема работы функции FEC

Чтобы включить функцию FEC:

1. Перейдите ко включению функции FEC одним из следующих способов:

   - Если вы хотите включить функцию FEC на соединении, установленном с устройства CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на нужное устройство CPE, выберите вкладку **Соединения** и нажмите на кнопку **Управление** → **FEC/реорганизация** рядом с соединением.

   - Если вы хотите включить функцию FEC на одном из соединений в таблице всех соединений, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Соединения** и нажмите на кнопку **Управление** → **FEC/реорганизация** рядом с соединением.

   - Если вы хотите включить функцию FEC на одном из соединений в графической топологии со всеми соединениями, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Топология**, нажмите на соединение и нажмите на кнопку **FEC/реорганизация**.

   - Если вы хотите включить функцию FEC на одном из соединений при создании интерфейса SD-WAN с типом WAN, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на нужное устройство CPE, выберите вкладку **SD-WAN** → **Интерфейсы,** в таблице интерфейсов SD-WAN нажмите на кнопку **+ Добавить** и выберите вкладку **Параметры соединений**.

2. В открывшемся окне включите переключатель **Переопределить**, чтобы переопределить параметры соединений.

   Этот переключатель выключен по умолчанию и не отображается, если вы настраиваете функцию FEC при создании интерфейса SD-WAN с типом WAN.

3. Включите функцию FEC на соединении с помощью переключателя **Включить FEC**. Этот переключатель выключен по умолчанию.

4. В раскрывающемся списке **Степень избыточности (исходные/дополнительные пакеты)** выберите соотношение между оригинальными пакетами трафика и дополнительными пакетами трафика с избыточным кодом. Значение по умолчанию: **0:0 (FEC выключен)** – функция FEC не используется. Вы также можете указать соотношение между оригинальными пакетами трафика и избыточными пакетами трафика с избыточным кодом с помощью свойства контроллера `topology.link.fec.ratio`.

5. В поле **Максимальное время в буфере реорганизации (мс)** введите время в миллисекундах, в течение которого пакет трафика может находиться в очереди для применения функции FEC. Диапазон значений: от 1 до 1000.

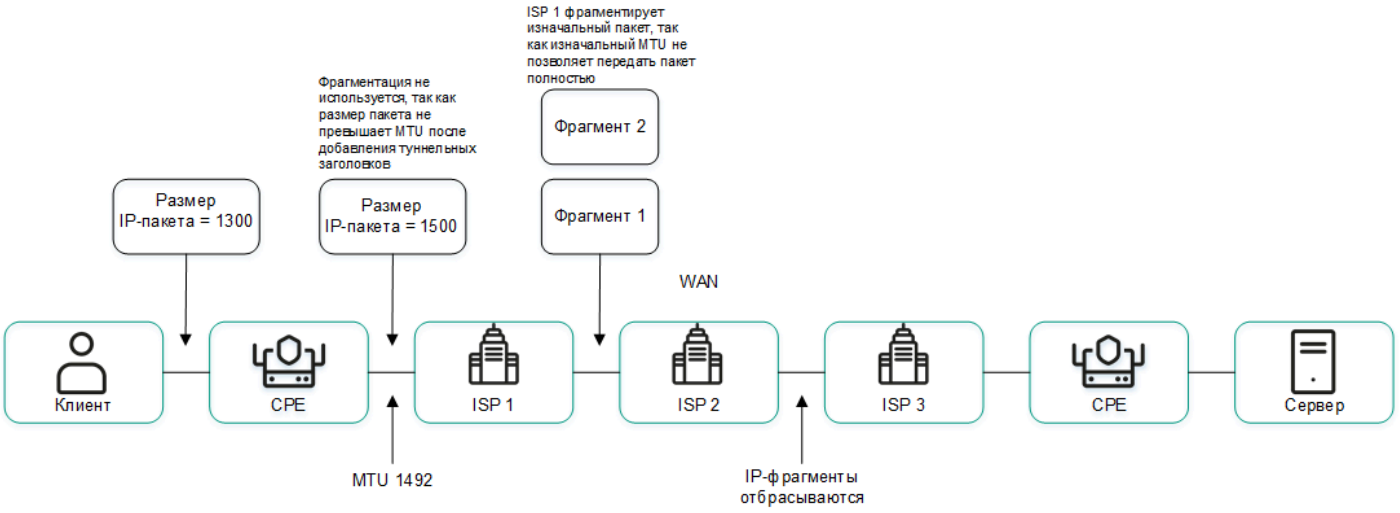
6. Нажмите на кнопку **Сохранить**.

   Функция FEC будет включена.

7. Если вы включили функцию FEC на соединении, установленном с устройства CPE, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Определение значения MTU

Вы можете определить значение MTU на соединении, чтобы понять, почему на соединении происходит блокирование фрагментированных пакетов (см. рисунок ниже).



Соединения с пониженным размером MTU и сбросом фрагментированных пакетов

Значение MTU определяется за счет отправки LLDP-пакетов с переменным размером полезной нагрузки (англ. payload) через соединение. Минимальный определяемый размер значения MTU составляет 1280 байт, максимальный – 1500 байт. Определение значения MTU происходит автоматически при включении устройств CPE, а также с интервалом времени, указанным с помощью свойства контроллера `topology.link.pmtud.scheduler.interval.sec`.

Вы можете определить значение MTU вручную.

Чтобы вручную определить значение MTU,

перейдите к определению значения MTU вручную одним из следующих способов:

- Если вы хотите вручную определить значение MTU на соединении, установленном с устройства CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Соединения** и нажмите на кнопку **Управление** → **Проверить MTU** рядом с соединением.

- Если вы хотите вручную определить значение MTU на одном из соединений в таблице всех соединений, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Соединения** и нажмите на кнопку **Управление** → **Проверить MTU** рядом с соединением.

Значение MTU отобразится в столбце **MTU**.

Шифрование трафика

Шифрование трафика – это механизм, обеспечивающий безопасную передачу трафика между устройствами CPE через соединения. Например, вы можете шифровать трафик, который передается через незащищенные соединения.

Шифрование трафика не отменяет необходимости использовать другие средства защиты информации, такие как TLS, LDAPS и другие протоколы, защищающие трафик внутри наложенной сети.

Контроллер автоматически генерирует ключи для шифрования и дешифровки трафика и передает их устройствам CPE. Трафик шифруется на устройстве CPE источника с помощью ключа для шифрования. Устройство CPE назначения дешифрует трафик с помощью ключа для дешифровки.

Используемые ключи регулярно обновляются, чтобы у третьих лиц не было возможности зашифровать или дешифровать передаваемый трафик при перехватывании ключа. Вы можете указать время, по прошествии которого ключи обновляются на устройствах CPE, с помощью свойства контроллера `topology.link.encryption.key.update.interval.minutes`.

Шифрование трафика поддерживается только на устройствах CPE с программным обеспечением Kaspersky SD-WAN.

Вы можете включить шифрование трафика на устройстве CPE или на соединении. Устройство CPE, на котором включено шифрование трафика, передает зашифрованный трафик через все свои соединения, включая новые соединения, которые будут построены позже. Когда шифрование трафика включено на соединении, устройство CPE передает зашифрованный трафик через соединение. При выключении шифрования трафика ключи, сгенерированные контроллером для шифрования и дешифровки трафика, удаляются со всех связанных устройств CPE. По умолчанию шифрование трафика выключено на устройствах CPE и соединениях.

Например, вы можете включить шифрование трафика на устройстве CPE и выключить шифрование трафика на одном из соединений устройства CPE. В этом случае устройство CPE будет передавать зашифрованный трафик через все свои соединения, за исключением соединения, на котором выключено шифрование трафика.

Включение шифрования трафика на устройстве CPE

Устройство CPE, на котором включено шифрование трафика, передает зашифрованный трафик через все свои соединения, включая новые соединения, которые будут построены позже. Вы можете включить шифрование трафика в шаблоне CPE или на устройстве CPE. Параметры шифрования трафика, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

Чтобы включить шифрование трафика на устройстве CPE:

1. Перейдите ко включению шифрования трафика на устройстве CPE одним из следующих способов:

   - Если вы хотите включить шифрование трафика в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **Шифрование соединения**.

   - Если вы хотите включить шифрование трафика на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Шифрование соединения** и установите флажок **Переопределить**.

   Отобразится политика шифрования трафика.

2. В раскрывающемся списке **Включить шифрование** выберите **Включено**. Значение по умолчанию: **Выключено**.

3. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Включение шифрования трафика на соединении

Когда шифрование трафика включено на соединении, устройство CPE передает зашифрованный трафик через соединение.

Чтобы включить шифрование трафика на соединении:

1. Перейдите ко включению шифрования трафика на соединении одним из следующих способов:

   - Если вы хотите включить шифрование трафика на соединении, установленном с устройства CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **Соединения** и нажмите на кнопку **Управление** → **Включить шифрование** рядом с соединением.

   - Если вы хотите включить шифрование трафика на одном из соединений в таблице всех соединений, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Соединения** и нажмите на кнопку **Управление** → **Включить шифрование** рядом с соединением.

   - Если вы хотите включить шифрование трафика на одном из соединений в графической топологии со всеми соединениями, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейдите в раздел **Топология**, нажмите на соединение и нажмите на кнопку **Включить шифрование**.

2. В открывшемся окне установите флажок **Переопределить**. Этот флажок снят по умолчанию.

3. Установите флажок **Включить шифрование**, чтобы включить шифрование трафика на соединении. Этот флажок снят по умолчанию.

4. Нажмите на кнопку **Сохранить**.

   Шифрование трафика будет включено на соединении.

5. Если вы включили шифрование трафика на соединении, установленном с устройства CPE, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Функция Connectivity Fault Management (CFM)

Функция *Connectivity Fault Management* (далее также CFM) позволяет обнаруживать недоступные соединения между устройствами CPE. Когда функция CFM включена, устройство CPE отправляет контрольные пакеты Continuity Check Message (CCM) через свои соединения с указанным вами интервалом времени и ожидает получения ответных контрольных пакетов через встречные соединения. При отсутствии ответных контрольных пакетов устройство CPE считает соединение недоступным и начинает передавать трафик по случайно выбранному доступному соединению.

Время ожидания ответных контрольных пакетов равняется интервалу времени для отправки контрольных пакетов, умноженному на 3.5. Время переключения устройства CPE на новое соединение при отсутствии ответных контрольных пакетов равняется интервалу времени для отправки контрольных пакетов, умноженному на число в диапазоне от 3.5 до 7. Например, если в качестве интервала времени для отправки контрольных пакетов указано 300 миллисекунд, время ожидания ответных контрольных пакетов составит 1.05 секунды, а время переключения устройства CPE на новое соединение при отсутствии ответных контрольных пакетов составит от 1.05 до 2.1 секунд.

> При использовании механизма CFM рекомендуется устанавливать интервал CFM и свойство контроллера `core.link.liveness.timeout` таким образом, чтобы выполнялось соотношение: `core.link.liveness.timeout` >= интервал CFM * 10.

Вы можете включить функцию CFM на устройстве CPE или соединении:

- Устройство CPE, на котором включена функция CFM, отправляет контрольные пакеты через все свои соединения, включая новые соединения, которые будут построены позже. Если вы указываете на устройствах CPE разные интервалы времени для отправки контрольных пакетов, используется самый большой из указанных интервалов времени. Например, если на устройстве CPE 1 в качестве интервала времени для отправки контрольных пакетов указано 300 миллисекунд, а на устройстве CPE 2 указана одна секунда, интервалом времени для отправки контрольных пакетов будет одна секунда.

  При включении функции CFM на одном устройстве CPE и выключении на другом устройстве CPE приоритет имеет устройство CPE со включенной функцией CFM. В этом случае устройства CPE отправляют друг другу контрольные пакеты через все свои соединения.

- Когда функция CFM включена на соединении, устройство CPE отправляет контрольные пакеты только через соединение. При включении функции CFM на соединении вам также нужно включить функцию CFM на встречном соединении. Интервал времени для отправки контрольных пакетов на соединении имеет приоритет перед интервалами времени для отправки контрольных пакетов на устройствах CPE. Например, если на устройстве CPE 1 в качестве интервала времени для отправки контрольных пакетов указано 300 миллисекунд, на устройстве CPE 2 указана одна секунда, а на соединении между устройствами CPE 1 и 2 указано десять секунд, интервалом времени для отправки контрольных пакетов будет десять секунд.

Например, вы можете включить функцию CFM на устройстве CPE и выключить функцию CFM на одном из соединений устройства CPE. В этом случае устройство CPE будет передавать контрольные пакеты через все свои соединения, за исключением соединения, на котором выключена функция CFM. По умолчанию функция CFM выключена на устройствах CPE и соединениях.

Изменение параметров CFM на активном соединении может вызвать перерыв трафика.

Включение функции CFM на устройстве CPE

Устройство CPE, на котором включена функция CFM, отправляет контрольные пакеты через все свои соединения, включая новые соединения, которые будут построены позже. Вы можете включить функцию CFM в шаблоне CPE или на устройстве CPE. Параметры функции CFM, указанные в шаблоне CPE, автоматически распространяются на все устройства CPE, которые используют шаблон CPE.

При включении функции CFM на одном устройстве CPE и выключении на другом устройстве CPE приоритет имеет устройство CPE со включенной функцией CFM. В этом случае устройства CPE отправляют друг другу контрольные пакеты через все свои соединения.

Изменение параметров CFM на активном соединении может вызвать перерыв трафика.

Чтобы включить функцию CFM на устройстве CPE:

1. Перейдите ко включению функции CFM на устройстве CPE одним из следующих способов:

   - Если вы хотите включить функцию CFM в шаблоне CPE, в меню перейдите в раздел **SD-WAN** → **Шаблоны CPE**, нажмите на шаблон CPE и выберите вкладку **CFM**.

   - Если вы хотите включить функцию CFM на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **CPE**, нажмите на устройство CPE, выберите вкладку **CFM** и установите флажок **Переопределить**.

2. В раскрывающемся списке **CFM** выберите **Включено**. Значение по умолчанию: **Выключено**.

3. В раскрывающемся списке **Интервал** выберите интервал времени для отправки контрольных пакетов:

   - **300 мс**.
   - **1 сек.**. Это значение выбрано по умолчанию.
   - **10 сек**.
   - **1 мин**.

   Время ожидания ответных контрольных пакетов равняется интервалу времени для отправки контрольных пакетов, умноженному на 3.5. Время переключения устройства CPE на новое соединение при отсутствии ответных контрольных пакетов равняется интервалу времени для отправки контрольных пакетов, умноженному на число в диапазоне от 3.5 до 7. Например, если в раскрывающемся списке **Интервал** выбрано **300 мс**, время ожидания ответных контрольных пакетов составит 1.05 секунды, а время переключения устройства CPE на новое соединение при отсутствии ответных контрольных пакетов составит от 1.05 до 2.1 секунд.

   Если вы указали разные интервалы времени для отправки контрольных пакетов на устройствах CPE, используется самый большой из указанных интервалов времени. Например, если на устройстве CPE 1 в раскрывающемся списке **Интервал** выбрано **300 мс**, а на устройстве CPE 2 выбрано **1 сек**, интервалом времени для отправки контрольных пакетов будет одна секунда.

4. В нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства CPE немедленно, или запланируйте отложенное сохранение параметров устройства CPE, нажав на значок ⌄ в правой части кнопки **Сохранить** и выбрав вариант **Запланированное сохранение**.

Включение функции CFM на соединении

Когда функция CFM включена на соединении, устройство CPE отправляет контрольные пакеты только через соединение. При включении функции CFM на соединении вам также нужно включить функцию CFM на встречном соединении.

Изменение параметров CFM на активном соединении может вызвать перерыв трафика.

Чтобы включить функцию CFM на соединении:

1. Перейдите ко включению функции CFM на соединении одним из следующих способов:

   - Если вы хотите включить функцию CFM на соединении, установленном с устройства CPE, в меню перейдите в раздел **SD-WAN → CPE**, нажмите на устройство CPE, выберите вкладку **Соединения** и нажмите на кнопку **Управление → Указать CFM** рядом с соединением.
   - Если вы хотите включить функцию CFM на одном из соединений в таблице всех соединений, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, перейдите в раздел **Соединения** и нажмите на кнопку **Управление → Указать CFM** рядом с соединением.

2. Если вы хотите включить функцию CFM на одном из соединений в графической топологии со всеми соединениями, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, перейдите в раздел **Топология**, нажмите на соединение и нажмите на кнопку **Указать CFM**.

3. В открывшемся окне установите флажок **Переопределить**. Этот флажок снят по умолчанию.

4. Установите флажок **Сохранить для обоих соединений**, чтобы включить функцию CFM на встречном соединении. Этот флажок снят по умолчанию.

5. В раскрывающемся списке **CFM** выберите **Включено**. Значение по умолчанию: **Выключено**.

6. В раскрывающемся списке **Интервал** выберите интервал времени для отправки контрольных пакетов:

   - **300 мс**.
   - **1 сек.**. Это значение выбрано по умолчанию.
   - **10 сек**.
   - **1 мин**.

   Время ожидания ответных контрольных пакетов равняется интервалу времени для отправки контрольных пакетов, умноженному на 3.5. Время переключения устройства CPE на новое соединение при отсутствии ответных контрольных пакетов равняется интервалу времени для отправки контрольных пакетов, умноженному на число в диапазоне от 3.5 до 7. Например, если в раскрывающемся списке **Интервал** выбрано **300 мс**, время ожидания ответных контрольных пакетов составит 1.05 секунды, а время переключения устройства CPE на новое соединение при отсутствии ответных контрольных пакетов составит от 1.05 до 2.1 секунд.

   Интервал времени для отправки контрольных пакетов на соединении имеет приоритет перед интервалами времени для отправки контрольных пакетов, которые вы указали при включении функции CFM на устройствах CPE. Например, если на устройстве CPE 1 в раскрывающемся списке **Интервал** выбрано **300 мс**, на устройстве CPE 2 выбрано **1 сек**, а на соединении между устройствами CPE 1 и 2 выбрано **10 сек**, интервалом времени для отправки контрольных пакетов будет 10 секунд.

7. Нажмите на кнопку **Сохранить**.

   Функция CFM будет включена на соединении.

8. Если вы включили функцию CFM на соединении, установленном с устройства CPE, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства CPE.

Работа с сегментами

Для просмотра таблицы сегментов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **Сегменты**. Информация о сегментах и входящих в них путях отображается в следующих столбцах таблицы:

- **От** – имя и идентификатор DPID устройства CPE источника сегмента.
- **До** – имя и идентификатор DPID устройства CPE назначения сегмента.
- **Пути/максимум** – количество построенных путей и максимальное количество путей, поддерживаемых сегментом.
- **#** – порядковый номер пути. Чем меньше порядковый номер пути, тем раньше путь был построен.

- **Тип пути** – тип пути:
  - **Auto SPF**.
  - **Auto TE**.
  - **Manual TE**.
- **Пути** – имена, идентификаторы DPID и номера OpenFlow-портов устройств CPE, через которые проходит путь.
- **Административное состояние** – административное состояние пути:
  - **работает**.
  - **не работает**.
- **Операционное состояние** – операционное состояние пути:
  - **работает**.
  - **не работает**.
- **Стоимость** – стоимость пути.
- **Количество хопов** – количество хопов в пути.
- **Вес для балансировки** – вес пути, рассчитанный на основе суммарной стоимости соединений.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание пути Manual-TE

При создании пути Manual-TE вам нужно вручную указать соединения, через которые он проходит от устройства CPE источника сегмента до устройства CPE назначения сегмента. Поддерживается создание двух типов путей Manual-TE:

- *Полностью определенный путь Manual-TE*, в котором указано каждое устройство CPE и сервисный интерфейс, через которые проходит путь Manual-TE.
- *Гибридный путь Manual-TE*, в котором указано одно или несколько устройств CPE и сервисных интерфейсов, через которые проходит путь Manual-TE. В этом случае между не указанными участками пути Manual-TE трафик передается автоматически (используется путь Auto-SPF).

Вы можете использовать ограничения Manual-TE, чтобы добавить пути Manual-TE в транспортные сервисы.

Примеры возможных путей Manual-TE:
В приведенных примерах после номера устройства CPE через двоеточие указан номер OpenFlow-порта.

Полностью определенный путь Manual-TE: CPE 1:3 → CPE 2:1, CPE 2:2 → CPE 4:1, CPE 4:5 → CPE N:2.

Гибридный путь Manual-TE: CPE 1 → CPE 5, CPE 5:3 → CPE 4:3, CPE 4 → CPE N. В этом случае путь от CPE 1 до CPE N строится как путь Auto-SPF CPE 1 →CPE 5, путь Manual-TE CPE 5:3 → CPE 4:3 и путь Auto-SPF CPE 4 → CPE N.

Чтобы создать путь Manual-TE:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сегменты**.

   Отобразится таблица сегментов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с сегментом, в котором вы хотите создать путь Manual-TE.

   Отобразятся параметры и таблица путей.

   Информация о путях отображается в следующих столбцах таблицы:

   - **Тип пути** – тип пути:
     - **Auto SPF**.
     - **Auto TE**.
     - **Manual TE**.
   - **Административное состояние** – административное состояние пути:
     - **работает**.
     - **не работает**.
   - **Операционное состояние** – операционное состояние пути:
     - **работает**.
     - **не работает**.
   - **Стоимость** – стоимость пути.
   - **Количество хопов** – количество хопов в пути.
   - **Балансировка нагрузки** – включена ли для пути балансировка нагрузки.
   - **Вес для балансировки** – вес пути для балансировки, рассчитанный на основе суммарной стоимости соединений.

5. Нажмите на кнопку **+ Путь Manual-TE**.

   Отобразятся параметры пути Manual-TE и таблица хопов.

   Информация о хопах отображается в следующих столбцах таблицы:

   - **#** – порядковый номер хопа. Чем меньше порядковый номер хопа, тем раньше хоп был добавлен.
   - **От** – имя, идентификатор DPID и номер OpenFlow-порта устройства CPE источника хопа.
   - **До** – имя, идентификатор DPID и номер OpenFlow-порта устройства CPE назначения хопа.
   - **Стоимость** – стоимость хопа.

   В верхней части таблицы отображается общая стоимость пути Manual-TE.

6. В поле **Имя** области настройки ведите имя пути Manual-TE.

7. В поле **Максимум хопов** введите максимальное количество хопов в пути Manual-TE. Диапазон значений: от 1 до 8. Значение по умолчанию: 4.

8. Добавьте хоп в путь Manual-TE:

   a. В раскрывающемся списке **От** слева выберите устройство CPE источника хопа.

      Если вы добавляете первый хоп в путь Manual-TE, в качестве устройства CPE источника хопа вы можете выбрать только устройство CPE источника сегмента. Если вы добавили хотя бы один хоп в путь Manual-TE, в качестве устройства CPE источника хопа вы можете выбрать только устройство CPE назначения предыдущего хопа.

   b. При необходимости в раскрывающемся списке **Порт** слева выберите OpenFlow-порт источника хопа. Значение по умолчанию: **Автоматически** – OpenFlow-порт определяется автоматически.

   c. В раскрывающемся списке **До** справа выберите устройство CPE назначения хопа.

      Если для устройства CPE источника хопа в раскрывающемся списке **Порт** выбрано значение **Автоматически**, в качестве устройства CPE назначения хопа вы можете выбрать любое устройство CPE, за исключением тех, что используются в других хопах. В этом случае для устройства CPE назначения хопа в раскрывающемся списке **Порт** выбирается значение **Автоматически** и OpenFlow-порт определяется автоматически. Таким образом, в хопе используется путь Auto-SPF.

      Если для устройства CPE источника хопа в раскрывающемся списке **Порт** выбран OpenFlow-порт, в качестве устройства CPE назначения хопа вы можете выбрать только устройство CPE, до которого от OpenFlow-порта построено соединение. В этом случае для устройства CPE назначения хопа в раскрывающемся списке **Порт** автоматически выбирается OpenFlow-порт, до которого построено соединение. Таким образом, в хопе используется соединение между двумя устройствами CPE.

   d. При необходимости в раскрывающемся списке **Порт** справа выберите OpenFlow-порт устройства CPE назначения хопа. Значение по умолчанию: **Автоматически** – OpenFlow-порт определяется автоматически.

   e. Нажмите на кнопку **Добавить**.

      Хоп будет добавлен и отобразится в таблице. Вы можете добавить несколько хопов и удалить хопы. Для удаления хопа выберите его в таблице и нажмите на кнопку **Удалить**.

9. Нажмите на кнопку **Создать**.

   Будет выполнена проверка, что устройство CPE назначения последнего хопа совпадает с устройством CPE назначения сегмента, в котором вы создаете путь Manual-TE. При успешной проверке путь Manual-TE будет создан и отобразится в таблице, а в столбце **Стоимость** отобразится стоимость пути Manual-TE, которая складывается из стоимости всех хопов, которые вы добавили в путь Manual-TE.

10. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры сегмента.

Изменение пути Manual-TE

Чтобы изменить путь Manual-TE:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сегменты**.

   Отобразится таблица сегментов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с сегментом, в котором вы хотите изменить путь Manual-TE.

   Отобразятся параметры и таблица путей.

5. Нажмите на кнопку **Изменить** рядом с путем Manual-TE, который вы хотите изменить.

   Отобразятся параметры пути Manual-TE и таблица хопов.

6. При необходимости измените параметры пути Manual-TE. Описание параметров см. в инструкции по созданию пути Manual-TE.

7. Нажмите на кнопку **Сохранить**.

   Путь Manual-TE будет изменен и обновится в таблице.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры сегмента.

Удаление пути Manual-TE

Удаленные пути Manual-TE невозможно восстановить.

Чтобы удалить путь Manual-TE:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сегменты**.

   Отобразится таблица сегментов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с сегментом, в котором вы хотите удалить путь Manual-TE.

   Отобразятся параметры и таблица путей.

5. Нажмите на кнопку **Удалить** рядом с путем Manual-TE, который вы хотите удалить.

   Путь Manual-TE будет удален и перестанет отображаться в таблице.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры сегмента.

Качество обслуживания (QoS)

Политика *качества обслуживания* (англ. Quality of Service, далее также QoS) обеспечивает передачу данных в соответствии с требованиями к классам трафика. В Kaspersky SD-WAN качество обслуживания складывается из следующих компонентов:

- Классы трафика – указывают приоритет обработки трафика и распределяют трафик по очередям. Например, вы можете использовать один из классов трафика для трафика реального времени, для которого требуется обеспечить минимальную потерю пакетов. Вы можете соотнести трафик с классами трафика при создании или изменении классификатора трафика.

- Классификаторы трафика – определяют, доверять или нет DSCP-значениям, указанным в полях заголовков пакетов трафика. Если классификатор трафика не доверяет DSCP-значениям, он соотносит их с классами трафика. Вы можете указать классификатор трафика при создании или изменении правила качества обслуживания, чтобы правило качества обслуживания использовало классификатор трафика.

- Правила качества обслуживания – определяют, ограничивается ли скорость трафика, обрабатываемого классификаторами трафика. Вы можете указать правило качества обслуживания при создании или изменении транспортного сервиса, чтобы транспортный сервис использовал правило качества обслуживания.

- Ограничения – используются для настройки построения путей в транспортных сервисах. Вы можете создать ограничения двух типов:

  - Ограничения Manual-TE – добавляют пути Manual-TE в транспортные сервисы.

  - Пороговые ограничения – указывают пороговые значения показателей мониторинга соединений, на основании которых строятся пути Auto-TE в транспортных сервисах.

  Вы можете указать ограничение при создании или изменении транспортного сервиса, чтобы транспортный сервис использовал ограничение.

- Правила классификации трафика – определяют в общем потоке данных трафик с указанными значениями полей заголовков L2-L4, а также трафик указанных приложений. Вы можете указать правило классификации трафика при создании или изменении фильтра трафика, чтобы фильтр трафика использовал правило классификации трафика.

- Фильтры трафика – фильтруют трафик на основании указанных правил классификации трафика. Вы можете указать фильтр трафика при создании или изменении транспортного сервиса или ACL-интерфейса, чтобы транспортный сервис или ACL-интерфейс использовал фильтр трафика.

Механизмы качества обслуживания

Политика качества обслуживания QoS позволяет классифицировать и управлять приоритетами обработки транзитного трафика между любыми интерфейсами CPE, включая интерфейсы типа bridge, интерфейсы SD-WAN, транспортные сервисы.

Схематично этапы применения инструментов качества обслуживания отображены на рис. 1

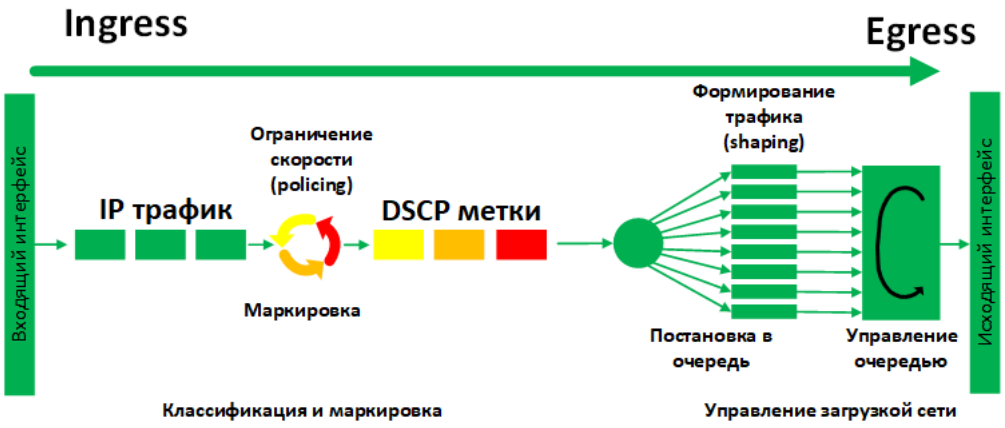


рис. 1 Инструменты качества обслуживания решения SD-WAN

Поступающий на входящий интерфейс трафик может быть маркирован на основании различных признаков для сопоставления с предопределенными классами трафика. Существующая маркировка входящего трафика также может быть изменена.

К маркированному трафику на входе может применяться механизм ограничения скорости (полисинг) в соответствии с классами трафика.

К маркированному трафику на выходе может применяться механизм формирования трафика (шейпинг) в соответствии с классами трафика.

Принцип действия этих механизмов отражен на рис. 2. Полисинг отбрасывает трафик, превышающий порог скорости передачи данных. Шейпинг сглаживает всплески трафика, внося дополнительную задержку.

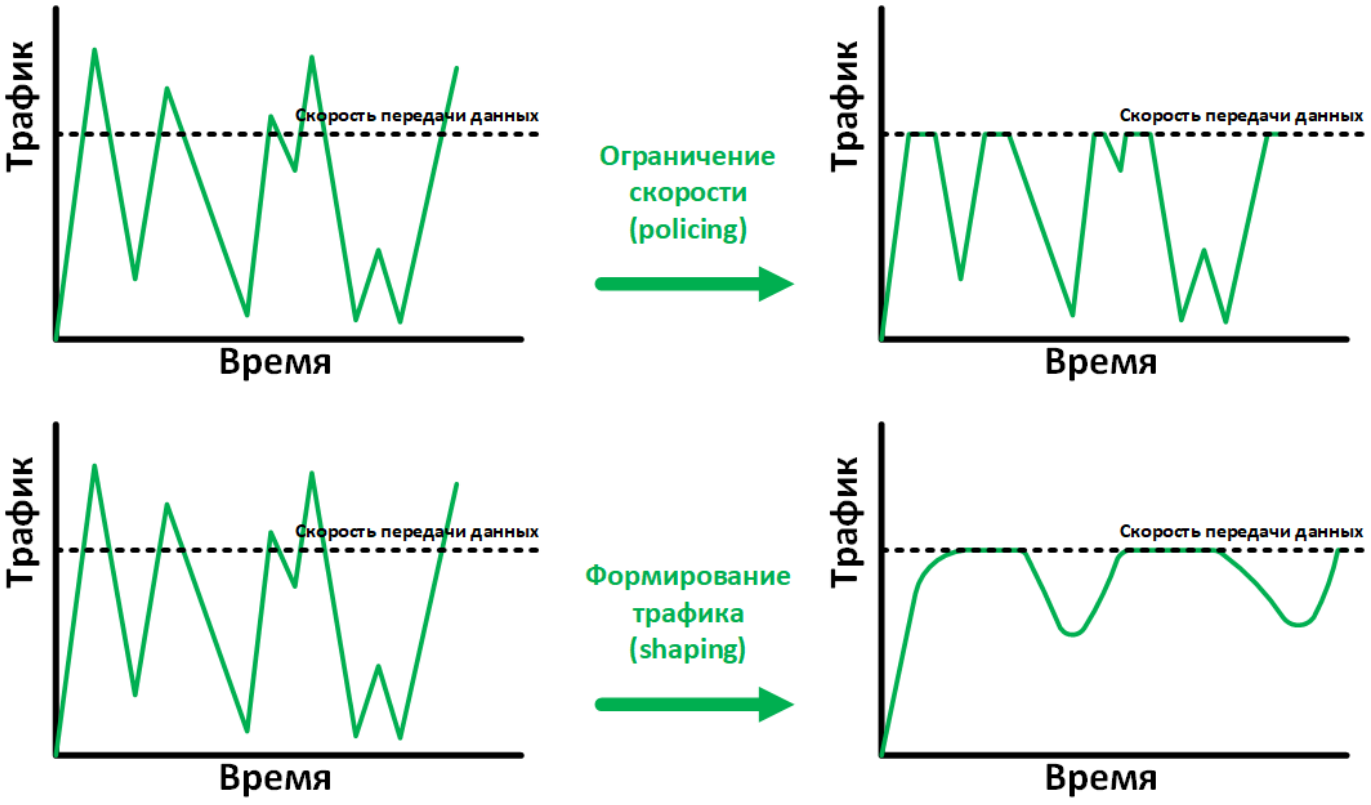


рис. 2 Механизмы обработки трафика

Маркировка и перемаркировка трафика

Маркировка с помощью CLASSIFY

Чтобы сопоставить трафик приложений подходящим классам трафика для последующей обработки механизмами качества обслуживания, можно воспользоваться функциональностью CLASSIFY расширенных правил межсетевого экрана.

На рис. 3 представлена схема обработки трафика межсетевым экраном в формате классического пакетного фильтра iptables. Функциональность CLASSIFY доступна в различных таблицах и цепочках.

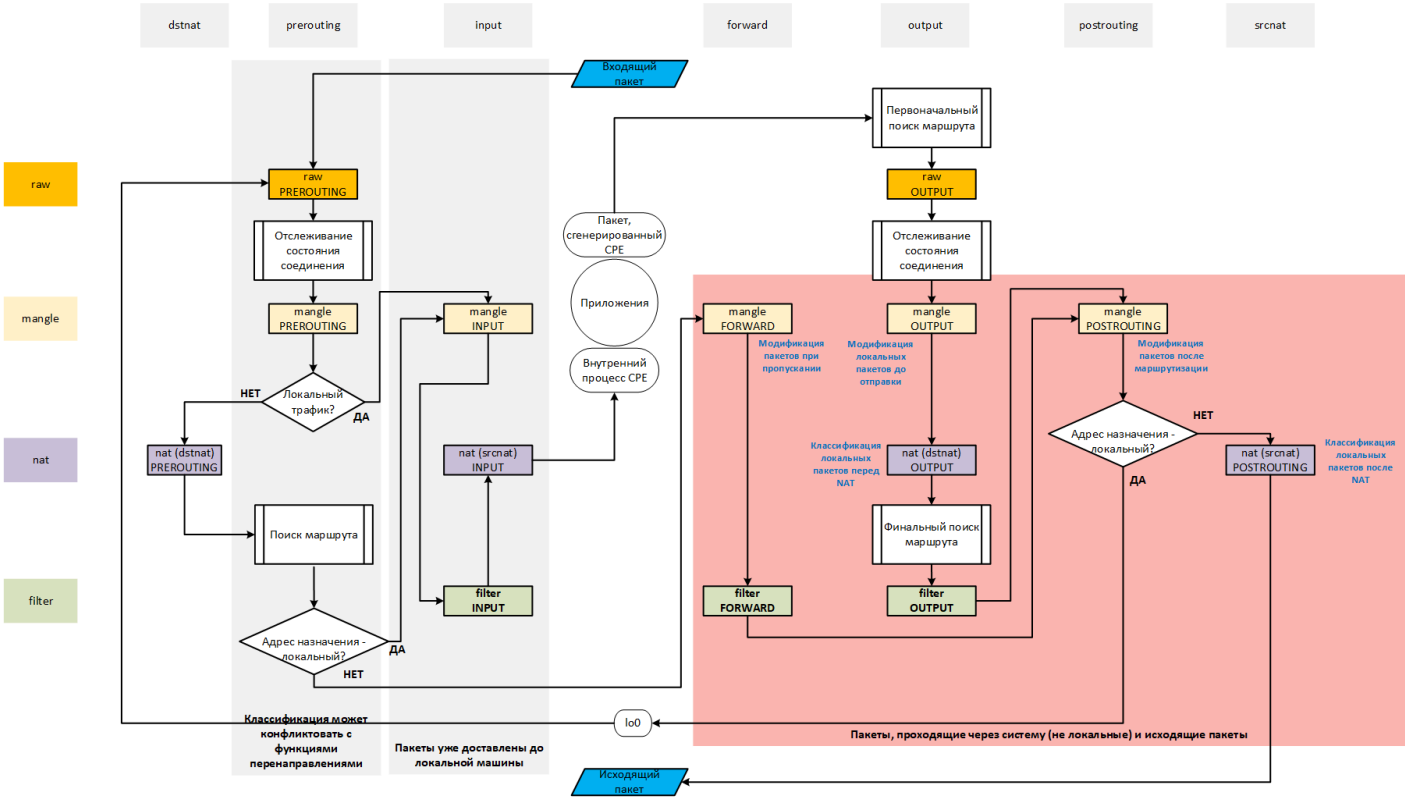


рис. 3 Точки классификации (CLASSIFY) расширенных правил межсетевого экрана

Для транзитного трафика рекомендуется использовать таблицу MANGLE, цепочку FORWARD.

Вы можете создать расширенное правило, выделяющее нужный вид трафика по различным критериям, в таблице MANGLE, цепочка FORWARD, действие CLASSIFY и сопоставить этому трафику нужную очередь (выбрать тэг очереди).

> Можно выбрать только очереди 0-6, что соответствует классам трафика Best Effort, Business Normal, Business Critical, Video, Conference, Signaling, Real Time. Поместить трафик приложений в очередь 7 (класс Network Control) нельзя.

Помеченный таким образом трафик помещается непосредственно в исходящую очередь. Это – полностью локальная маркировка, которая используется только внутри CPE для распределения трафика по очередям.

Маркировка с помощью TOS

Кроме этого, можно маркировать или перемаркировать входящий трафик для его сопоставления с заданными классами трафика с помощью действия TOS расширенных правил межсетевого экрана.

В отличие от маркировки CLASSIFY, TOS/DSCP значения - это часть IP-заголовка, они видимы за пределами устройства и могут влиять на маршрутизацию и приоритет в сетях.

Маркировки DSCP и TOS, соответствующие преднастроенным классам трафика, приведены в таблице ниже.

Маркировки DSCP и TOS, соответствующие преднастроенным классам трафика

Тег класса трафика	Очередь	маркировка DSCP	маркировка TOS
0	Best Effort	BE	0
1	Business Normal	CS1	32
2	Business Critical	CS2	64
3	Signaling	AF21	72
4	Video	AF42	144
5	Conference	EF	184
6	Real Time	AF22	80

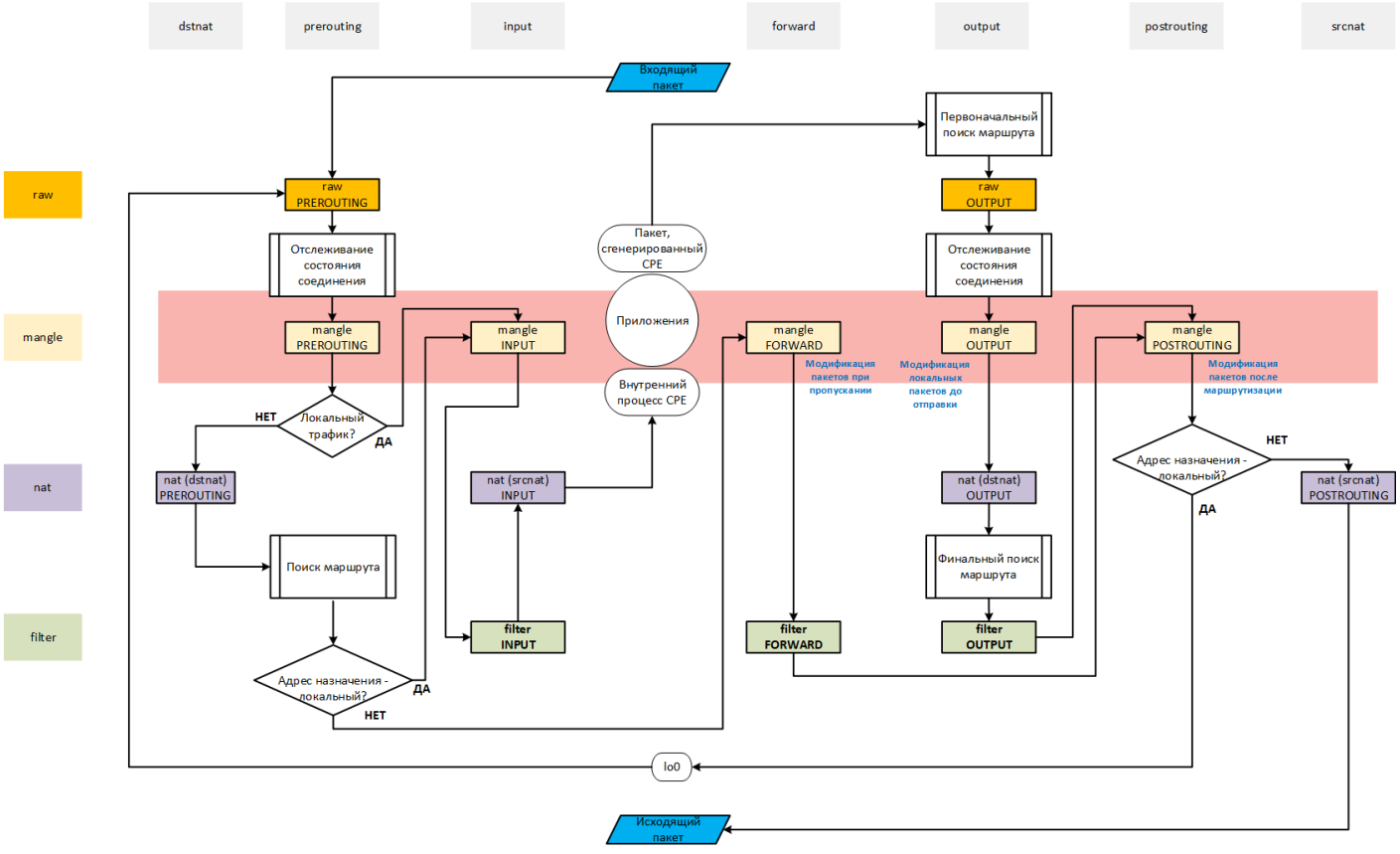


рис. 4 Точки маркировки (TOS) расширенных правил межсетевого экрана

Детальная схема применения механизмов качества обслуживания решения SD-WAN с учетом наложенных сетей приведена на рис. 5.

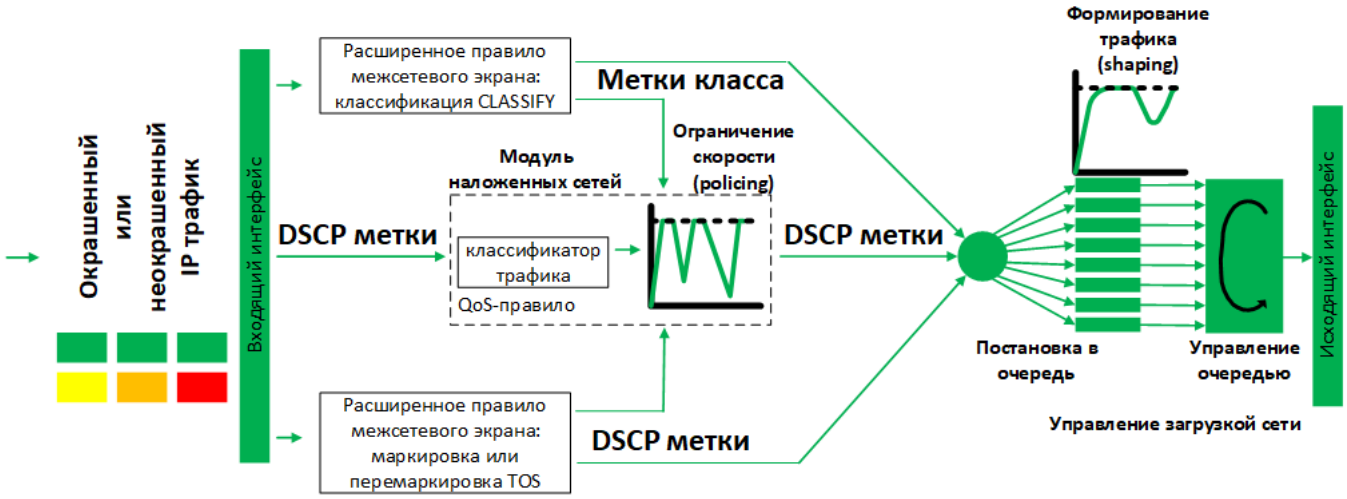


рис. 5 Инструменты качества обслуживания решения SD-WAN - детально

Формирование трафика (шейпинг)

Функция формирования трафика включается отдельно для каждого интерфейса.

Для настройки формирования трафика на основании меток класса или меток DSCP на физических или логических интерфейсах устройства CPE, перейдите в меню оркестратора CPE, выберите устройство, далее перейдите в пункт меню Сеть → нужный интерфейс → вкладка «QoS».

Переключите «Включено» в состояние «Да».

Здесь же можно отредактировать параметры общей скорости на интерфейсе и параметры минимальной и максимальной полосы каждого класса трафика.

Для настройки формирования трафика на основании меток класса или меток DSCP на физических или логических интерфейсах в шаблоне CPE, перейдите в меню оркестратора Шаблоны CPE, выберите шаблон, далее перейдите в пункт меню Сеть → нужный интерфейс → вкладка «QoS».

Переключите «Включено» в состояние «Да».

Здесь же можно отредактировать параметры общей скорости на интерфейсе и параметры минимальной и максимальной полосы каждого класса трафика.

QoS для интерфейсов sdwan включен всегда, а параметры скорости можно отредактировать в меню SDWAN выбранного устройства CPE или шаблона CPE, интерфейс типа sdwan, вкладка QoS.

Работа с классами трафика

О классах трафика

Вы можете посмотреть таблицу классов трафика в шаблоне экземпляра SD-WAN и меню настройки контроллера:

- Для просмотра таблицы классов трафика в шаблоне экземпляра SD-WAN вам нужно в меню перейти в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажать на шаблон экземпляра SD-WAN и выбрать вкладку **Классы трафика**.

- Для просмотра таблицы классов трафика в меню настройки контроллера вам нужно в меню перейти в раздел **Инфраструктура**, открыть параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, и перейти в раздел **QoS**.

По умолчанию созданы следующие классы трафика:

- **Best effort**.
- **Business normal**.
- **Business critical**.
- **Video**.
- **Conference**.
- **Signaling**.
- **Real time**.
- **Network control**.

Информация о классах трафика отображается в следующих столбцах таблицы:

- **Имя** – имя класса трафика.
- **Тег класса** – внутренний тег класса трафика.
- **Номер очереди** – номер очереди, в которую помещается трафик из класса трафика.
- **KOver** – коэффициент переподписки скорости передачи трафика, который определяет, во сколько раз может быть увеличена указанная для класса трафика скорость, если общая скорость используется не полностью.
- **Исключить при расчете пути** – скорость, доступная классу трафика, учитывается при расчете маршрута:
  - **Да**.
  - **Нет**.

В нижней части таблицы отображаются следующие параметры:

- **Класс трафика по умолчанию** – класс трафика, в который помещается трафик, не попавший в другие классы трафика.
- **Класс управляющего трафика** – класс трафика, в который помещается управляющий трафик который используется для управления компонентами решения. Мы рекомендуем назначить управляющему трафику наиболее высокий приоритет для надежного функционирования сети.
- **Максимальная зарезервированная скорость (%)** – процент максимальной скорости передачи трафика, который может быть доступен для класса трафика.

Kaspersky SD-WAN не поддерживает создание классов трафика, но вы можете изменить классы трафика по умолчанию в шаблоне экземпляра SD-WAN или меню настройки контроллера.

Изменение класса трафика

Вы можете изменить класс трафика в шаблоне экземпляра SD-WAN или меню настройки контроллера. Если вы изменяете класс трафика в шаблоне экземпляра SD-WAN, класс трафика не изменяется в меню настройки контроллера уже развернутых экземпляров SD-WAN.

> Классы трафика по умолчанию подходят для большинства схем развертывания решения, и мы не рекомендуем изменять их.

Чтобы изменить класс трафика:

1. Перейдите к изменению класса трафика одним из следующих способов:
   - Если вы хотите изменить класс трафика в шаблоне экземпляра SD-WAN, в меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажмите на шаблон экземпляра SD-WAN и выберите вкладку **Классы трафика**.
   - Если вы хотите изменить класс трафика в меню настройки контроллера, в меню перейдите в раздел **Инфраструктура**, откройте параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, и перейти в раздел **QoS**.

   Отобразится таблица классов трафика.
2. Нажмите на кнопку **Изменить**.
3. В столбце **Имя** укажите имя класса трафика.
4. В столбце **Номер очереди** выберите номер очереди, в которую помещается трафик из класса. Чем выше указанное значение, тем выше приоритет класса трафика. Вы не можете указать одинаковый приоритет для нескольких классов трафика.
5. В столбце **KOver** выберите коэффициент переподписки скорости передачи трафика, который определяет, во сколько раз может быть увеличена определенная для класса трафика скорость, если общая скорость используется не полностью.
6. Если вы хотите не учитывать доступную классу трафика скорость при построении пути, установите флажок **Исключить при расчете пути**. Когда флажок установлен, вы не можете выбрать для класса трафика коэффициент **KOver**. Этот флажок установлен рядом с классом трафика **Best effort** по умолчанию.

7. В раскрывающемся списке **Класс трафика по умолчанию** выберите класс трафика, в который помещается трафик, не попавший в другие классы трафика. По умолчанию выбран класс трафика **Best effort**.

8. В раскрывающемся списке **Класс управляющего трафика** выберите класс трафика, в который помещается управляющий трафик. По умолчанию выбран класс трафика **Network control**.

9. В раскрывающемся списке **Максимальная зарезервированная скорость (%)** выберите процент максимальной скорости передачи трафика, который может быть доступен для класса трафика. Диапазон значений: от 10 до 90. Значение по умолчанию: **90**.

10. Нажмите на кнопку **Сохранить**.

    Класс трафика будет изменен.

Работа с классификаторами трафика

Вы можете посмотреть таблицу классификаторов трафика в шаблоне экземпляра SD-WAN и меню настройки контроллера:

- Для просмотра таблицы классификаторов трафика в шаблоне экземпляра SD-WAN вам нужно в меню перейти в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажать на шаблон экземпляра SD-WAN и выбрать вкладку **Классификаторы**.

- Для просмотра таблицы классификаторов трафика в меню настройки контроллера вам нужно в меню перейти в раздел **Инфраструктура**, открыть параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, перейти в раздел **QoS** и выбрать вкладку **Классификаторы**.

По умолчанию создан классификатор трафика **Untrust-BE-Classifier**, который не доверяет DSCP-значениям в полях заголовков пакетов трафика и помещает весь трафик в класс трафика **Best effort**. Информация о классах трафика отображается в следующих столбцах таблицы:

- **Имя** – имя классификатора трафика.

- **Тип** – классификатор трафика доверяет DSCP-значениям в полях заголовков пакетов трафика:

  - **Да**.

  - **Нет**.

- **Класс трафика** – классы трафика, в который классификатор трафика помещает трафик.

- **Поле пакета** – заголовки пакетов трафика.

- **Внешняя метка** – DSCP-значения, которые должны содержать заголовки пакетов трафика, чтобы классификатор трафика помещал трафик в класс трафика.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание классификатора трафика

Вы можете создать классификатор трафика в шаблоне экземпляра SD-WAN или меню настройки контроллера. Если вы создаете классификатор трафика в шаблоне экземпляра SD-WAN, классификатор трафика не создается в меню настройки контроллера уже развернутых экземпляров SD-WAN.

Чтобы создать классификатор трафика:

1. Перейдите к созданию классификатора трафика одним из следующих способов:

   - Если вы хотите создать классификатор трафика в шаблоне экземпляра SD-WAN, в меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажмите на шаблон экземпляра SD-WAN и выберите вкладку **Классификаторы**.

   - Если вы хотите создать классификатор трафика в меню настройки контроллера, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, перейдите в раздел **QoS** и выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

2. Нажмите на кнопку **+ Классификатор**.

3. В открывшемся окне в поле **Имя** введите имя классификатора трафика.

4. В списке **Тип** выберите одно из следующих значений:

   - **Trust** – классификатор трафика доверяет DSCP-значениям в полях заголовков пакетов трафика. Это значение выбрано по умолчанию.

   - **Untrust** – классификатор трафика не доверяет DSCP-значениям в полях заголовков пакетов трафика.

5. Если в списке **Тип** вы выбрали **Trust**, установите соответствие между классами трафика и DSCP-значениями в полях заголовков пакетов трафика:

   a. В столбце **Класс трафика** выберите класс трафика, в который классификатор трафика помещает трафик.

   b. В столбце **Внешняя метка** нажмите на кнопку **Выбрать** рядом с полем заголовка пакетов трафика.

   c. Установите флажки рядом с отобразившимися DSCP-значениями, которые должны быть в поле заголовка пакетов трафика, чтобы классификатор трафика помещал трафик в класс трафика.

   d. Нажмите на кнопку **Ок**.

6. Если в списке **Тип** вы выбрали **Untrust**, в раскрывающемся списке **Класс трафика** выберите класс трафика, в который классификатор трафика помещает весь трафик.

7. Нажмите на кнопку **Создать**.

   Классификатор трафика будет создан и отобразится в таблице.

8. Если вы создали классификатор трафика в шаблоне экземпляра SD-WAN, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Вы можете указать классификатор трафика при создании или изменении правила качества обслуживания, чтобы правило качества обслуживания использовало классификатор трафика.

Изменение классификатора трафика

Вы можете изменить классификатор трафика в шаблоне экземпляра SD-WAN или меню настройки контроллера. Если вы изменяете классификатор трафика в шаблоне экземпляра SD-WAN, классификатор трафика не изменяется в меню настройки контроллера уже развернутых экземпляров SD-WAN.

Чтобы изменить классификатор трафика:

1. Перейдите к изменению классификатора трафика одним из следующих способов:

   - Если вы хотите изменить классификатор трафика в шаблоне экземпляра SD-WAN, в меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажмите на шаблон экземпляра SD-WAN и выберите вкладку **Классификаторы**.

   - Если вы хотите изменить классификатор трафика в меню настройки контроллера, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, перейдите в раздел **QoS** и выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

2. Нажмите на кнопку **Управление → Изменить** рядом с классификатором трафика, который вы хотите изменить.

3. В открывшемся окне при необходимости измените параметры классификатора трафика. Описание параметров см. в инструкции по созданию классификатора трафика.

4. Нажмите на кнопку **Сохранить**.

   Классификатор трафика будет изменен и обновится в таблице.

5. Если вы изменили классификатор трафика в шаблоне экземпляра SD-WAN, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Удаление классификатора трафика

Вы можете удалить классификатор трафика в шаблоне экземпляра SD-WAN или меню настройки контроллера. Если вы удаляете классификатор трафика в шаблоне экземпляра SD-WAN, классификатор трафика не удаляется в меню настройки контроллера уже развернутых экземпляров SD-WAN.

Удаленные классификаторы трафика невозможно восстановить.

Чтобы удалить классификатор трафика:

1. Перейдите к удалению классификатора трафика одним из следующих способов:

   - Если вы хотите удалить классификатор трафика в шаблоне экземпляра SD-WAN, в меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажмите на шаблон экземпляра SD-WAN и выберите вкладку **Классификаторы**.

   - Если вы хотите удалить классификатор трафика в меню настройки контроллера, в меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Параметры развертывания** рядом с контроллером, перейдите в раздел **QoS** и выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

2. Нажмите на кнопку **Управление → Удалить** рядом с классификатором трафика, который вы хотите удалить.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Классификатор трафика будет удален и перестанет отображаться в таблице.

4. Если вы удалили классификатор трафика в шаблоне экземпляра SD-WAN, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Работа с правилами качества обслуживания

Вы можете посмотреть таблицу правил качества обслуживания в шаблоне экземпляра SD-WAN и меню настройки контроллера:

- Для просмотра таблицы правил качества обслуживания в шаблоне экземпляра SD-WAN вам нужно в меню перейти в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажать на шаблон экземпляра SD-WAN и выбрать вкладку **QoS-правила**.

- Для просмотра таблицы правил качества обслуживания в меню настройки контроллера вам нужно в меню перейти в раздел **Инфраструктура**, открыть параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, затем перейти в раздел **QoS** и выбрать вкладку **QoS-правила**.

По умолчанию создано правило качества обслуживания **Unlimited-QoS**, которое использует классификатор трафика по умолчанию **Untrust-BE-Classifier**, не ограничивает скорость передачи трафика и предоставляет классу трафика **Best effort** 100% от общей скорости передачи трафика. Информация о правилах качества обслуживания отображается в следующих столбцах таблицы:

- **Имя** – имя правила качества обслуживания.
- **MBR** – максимальная скорость передачи трафика, разрешенная правилом качества обслуживания.
- В следующих столбцах отображается процент от общей скорости передачи трафика, доступный классам трафика:
  - **Best effort**.
  - **Business normal**.
  - **Business critical**.
  - **Video**.
  - **Conference**.
  - **Signaling**.
  - **Real time**.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание правила качества обслуживания

Вы можете создать правило качества обслуживания в шаблоне экземпляра SD-WAN или меню настройки контроллера. Если вы создаете правило качества обслуживания в шаблоне экземпляра SD-WAN, правило качества обслуживания не создается в меню настройки контроллера уже развернутых экземпляров SD-WAN.

Чтобы создать правило качества обслуживания:

1. Перейдите к созданию правила качества обслуживания:
   - Если вы хотите создать правило качества обслуживания в шаблоне экземпляра SD-WAN, в меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажмите на шаблон экземпляра SD-WAN и выберите вкладку **QoS-правила**.
   - Если вы хотите создать правило качества обслуживания в меню настройки контроллера, в меню перейдите в раздел **Инфраструктура**, откройте параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, перейдите в раздел **QoS** и выберите вкладку **QoS-правила**.

   Отобразится таблица правил качества обслуживания.
2. Нажмите на кнопку **+ QoS-правило**.
3. В открывшемся окне в поле **Имя** введите имя правила качества обслуживания.

4. В раскрывающемся списке **Классификатор** выберите созданный классификатор трафика, который вы хотите использовать в правиле качества обслуживания.

5. Если вы хотите, чтобы правило качества обслуживания ограничивало скорость передачи трафика, обрабатываемого классификатором трафика, снимите флажок **Не ограничено**. Этот флажок установлен по умолчанию.

6. Если вы сняли флажок **Не ограничено**, настройте ограничение скорости трафика:

   a. В поле **MBR** введите максимальную скорость передачи трафика (англ. Maximum Bit Rate). Значение по умолчанию: `1`.

   b. В раскрывающемся списке **Тип скорости** выберите единицы измерения максимальной скорости передачи трафика:

      - **Кбит/сек**. Это значение выбрано по умолчанию.
      - **Мбит/сек**.
      - **Гбит/сек**.

   c. Если в раскрывающемся списке **Классификатор** вы выбрали классификатор трафика с типом **Trust**, в столбце **Максимальная зарезервированная скорость (%)** укажите процент от общей скорости передачи трафика, доступный классам трафика. Сумма указанных значений должна быть равна 100%.

7. Нажмите на кнопку **Создать**.

   Правило качества обслуживания будет создано и отобразится в таблице.

8. Если вы создали правило качества обслуживания в шаблоне экземпляра SD-WAN, в нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Вы можете указать правило качества обслуживания при создании или изменении транспортного сервиса, чтобы транспортный сервис использовал правило качества обслуживания.

Изменение правила качества обслуживания

Вы можете изменить правило качества обслуживания в шаблоне экземпляра SD-WAN или меню настройки контроллера. Если вы изменяете правило качества обслуживания в шаблоне экземпляра SD-WAN, правило качества обслуживания не изменяется в меню настройки контроллера уже развернутых экземпляров SD-WAN.

Чтобы изменить правило качества обслуживания:

1. Перейдите к изменению правила качества обслуживания:

   - Если вы хотите изменить правило качества обслуживания в шаблоне экземпляра SD-WAN, в меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажмите на шаблон экземпляра SD-WAN и выберите вкладку **QoS-правила**.

   - Если вы хотите изменить правило качества обслуживания в меню настройки контроллера, в меню перейдите в раздел **Инфраструктура**, откройте параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, перейдите в раздел **QoS** и выберите вкладку **QoS-правила**.

   Отобразится таблица правил качества обслуживания.

2. Нажмите на имя правила качества обслуживания, которое вы хотите изменить, или выберите его в таблице и нажмите на кнопку **Изменить**.

3. В открывшемся окне при необходимости измените параметры качества обслуживания. Описание параметров см. в инструкции по созданию правила качества обслуживания.

4. Нажмите на кнопку **Сохранить**.

   Правило качества обслуживания будет изменено и обновится в таблице.

5. Если вы изменили правило качества обслуживания в шаблоне экземпляра SD-WAN, в нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Удаление правила качества обслуживания

Вы можете удалить правило качества обслуживания в шаблоне экземпляра SD-WAN или меню настройки контроллера. Если вы удаляете правило качества обслуживания трафика в шаблоне экземпляра SD-WAN, правило качества обслуживания не удаляется в меню настройки контроллера уже развернутых экземпляров SD-WAN.

Удаленные правила качества обслуживания невозможно восстановить.

Чтобы удалить правило качества обслуживания:

1. Перейдите к удалению правила качества обслуживания:

   - Если вы хотите удалить правило качества обслуживания в шаблоне экземпляра SD-WAN, в меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажмите на шаблон экземпляра SD-WAN и выберите вкладку **QoS-правила**.

   - Если вы хотите удалить правило качества обслуживания в меню настройки контроллера, в меню перейдите в раздел **Инфраструктура**, откройте параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, перейдите в раздел **QoS** и выберите вкладку **QoS-правила**.

   Отобразится таблица правил качества обслуживания.

2. Выберите правило качества обслуживания, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Правило качества обслуживания будет удалено и перестанет отображаться в таблице.

4. Если вы удалили правило качества обслуживания в шаблоне экземпляра SD-WAN, в нижней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Работа с ограничениями Manual-TE

Для просмотра таблицы ограничений Manual-TE вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление → Параметры развертывания** рядом с контроллером и перейти в раздел **Ограничения**. Информация об ограничениях Manual-TE отображается в следующих столбцах таблицы:

- **Имя** – имя ограничения Manual-TE.
- **Сегмент** – сегмент, к которому относятся пути Manual-TE, добавленные в ограничение Manual-TE.
- **Пути** – пути Manual-TE, которые были добавлены в ограничение Manual-TE.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание ограничения Manual-TE

Чтобы создать ограничение Manual-TE:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   По умолчанию выбрана вкладка **Manual-TE**, на которой отображается таблица ограничений Manual-TE.

4. В верхней части страницы нажмите на кнопку **+ Добавить**.

5. В открывшемся окне в поле **Имя** введите имя ограничения Manual-TE.

6. Установите флажок **Использовать путь Manual-TE** рядом с созданными путями Manual-TE, которые вы хотите добавить в ограничение Manual-TE. По умолчанию флажки сняты.

7. Если вы хотите разрешить использование пути Auto-SPF при недоступности указанных путей Manual-TE, установите флажок **Игнорировать, если путь с ограничением не найден** рядом с путями Manual-TE. Вы можете установить флажок только рядом с путями Manual-TE, рядом с которыми установлен флажок **Использовать путь Manual-TE**. По умолчанию флажки сняты.

8. Нажмите на кнопку **Создать**.

Ограничение Manual-TE будет создано и отобразится в таблице.

Вы можете указать ограничение Manual-TE при создании или изменении транспортного сервиса, чтобы транспортный сервис использовал ограничение Manual-TE.

Изменение ограничения Manual-TE

Чтобы изменить ограничение Manual-TE:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   По умолчанию выбрана вкладка **Manual-TE**, на которой отображается таблица ограничений Manual-TE.

4. Нажмите на имя ограничения Manual-TE, которое вы хотите изменить, или выберите его в таблице и нажмите на кнопку **Изменить**.

5. В открывшемся окне при необходимости измените параметры ограничения Manual-TE. Описание параметров см. в инструкции по созданию ограничения Manual-TE.

6. Нажмите на кнопку **Сохранить**.

Ограничение Manual-TE будет изменено и обновится в таблице.

Удаление ограничения Manual-TE

Удаленные ограничения Manual-TE невозможно восстановить.

Чтобы удалить ограничение Manual-TE:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   По умолчанию выбрана вкладка **Manual-TE**, на которой отображается таблица ограничений Manual-TE.

4. Выберите в таблице ограничение Manual-TE, которое вы хотите удалить и нажмите на кнопку **Удалить**.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Ограничение Manual-TE будет удалено и перестанет отображаться в таблице.

Работа с пороговыми ограничениями

Для просмотра таблицы пороговых ограничений вам нужно в меню перейти в раздел **Инфраструктура**, открыть параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, затем перейти в раздел **Ограничения** и выбрать вкладку **Пороговые ограничения**. Информация о пороговых ограничениях отображается в следующих столбцах таблицы:

- **Имя** – имя порогового ограничения.
- **Последний вариант** – пороговое ограничение исключает соединение из расчета пути Auto-TE, если в параметрах мониторинга соединения установлен флажок **Последний вариант**:
  - **Y**.
  - **N**.
- **Уровень ошибок** – пороговое ограничение исключает соединение из расчета пути Auto-TE, если на соединении достигнуто пороговое значение количества ошибок в секунду:
  - **Y**.
  - **N**.

- **Использование** – пороговое ограничение исключает соединение из расчета пути Auto-TE, если на соединении достигнуто пороговое значение загруженности в процентах от скорости сервисного интерфейса источника:
  - **Y**.
  - **N**.
- **Задержка** – пороговое ограничение исключает соединение из расчета пути Auto-TE, если на соединении достигнуто пороговое значение времени задержки в миллисекундах при передаче трафика через соединение:
  - **Y**.
  - **N**.
- **Джиттер** – пороговое ограничение исключает соединение из расчета пути Auto-TE, если на соединении достигнуто пороговое значение времени джиттера в миллисекундах при передаче трафика через соединение:
  - **Y**.
  - **N**.
- **Потеря пакетов** – пороговое ограничение исключает соединение из расчета пути Auto-TE, если на соединении достигнуто пороговое значение процента потерь пакетов трафика:
  - **Y**.
  - **N**.

Вы можете указать пороговые значения показателей мониторинга при настройке мониторинга соединений.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание порогового ограничения

Чтобы создать пороговое ограничение:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   По умолчанию выбрана вкладка **Manual-TE**, на которой отображается таблица ограничений Manual-TE.

4. Выберите вкладку **Пороговые ограничения**.

   Отобразится таблица пороговых ограничений.

5. В верхней части страницы нажмите на кнопку **+ Пороговое ограничение**.

6. В открывшемся окне в поле **Имя** введите имя порогового ограничения.

7. Установите флажок **Не использовать соединения с пороговым значением** рядом с показателями мониторингга соединений, чтобы пороговое ограничение исключало из расчета пути Auto-TE соединения, на которых достигнуто пороговое значение показателей мониторинга. Этот флажок снят по умолчанию.

8. Если вы хотите, чтобы пороговое ограничение не исключало из расчета пути Auto-TE соединения, на которых достигнуто пороговое значение указанных показателей мониторинга при отсутствии альтернативных соединений, установите флажок **Игнорировать, если путь с ограничением не найден** рядом с показателями мониторинга. Этот флажок снят по умолчанию. Вы можете установить флажок только рядом с показателями мониторинга, рядом с которыми установлен флажок **Не использовать соединения с пороговым значением**.

   Например, если вы установили флажок **Не использовать соединения с пороговым значением** рядом с показателем мониторинга **Уровень ошибок**, пороговое ограничение исключает из расчета пути Auto-TE соединение, на котором достигнуто пороговое значение количества ошибок в секунду. Если вы также установили флажок **Игнорировать, если путь с ограничением не найден** и на всех соединениях достигнуто пороговое значение количества ошибок в секунду, пороговое ограничение не исключает соединение из расчета пути Auto-TE.

9. Нажмите на кнопку **Создать**.

Пороговое ограничение будет создано отобразится в таблице.

Вы можете указать пороговое ограничение при создании или изменении транспортного сервиса, чтобы транспортный сервис использовал пороговое ограничение.

Изменение порогового ограничения

Чтобы изменить пороговое ограничение:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   По умолчанию выбрана вкладка **Manual-TE**, на которой отображается таблица ограничений Manual-TE.

4. Выберите вкладку **Пороговые ограничения**.

   Отобразится таблица пороговых ограничений.

5. Нажмите на имя порогового ограничения, которое вы хотите изменить, или выберите его в таблице и нажмите на кнопку **Изменить**.

6. В открывшемся окне при необходимости измените параметры порогового ограничения. Описание параметров см. в инструкции по созданию порогового ограничения.

7. Нажмите на кнопку **Сохранить**.

Пороговое ограничение будет изменено и обновится в таблице.

Удаление порогового ограничения

Удаленные пороговые ограничения невозможно восстановить.

Чтобы удалить пороговые ограничения:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   По умолчанию выбрана вкладка **Manual-TE**, на которой отображается таблица ограничений Manual-TE.

4. Выберите вкладку **Пороговые ограничения**.

   Отобразится таблица пороговых ограничений.

5. Выберите в таблице пороговое ограничение, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

6. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Пороговое ограничение будет удалено и перестанет отображаться в таблице.

Работа с правилами классификации трафика

Для просмотра таблицы правил классификации трафика вам нужно в меню перейти в раздел **Инфраструктура**, открыть параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, затем перейти в раздел **Фильтры трафика**.

Информация о правилах классификации трафика отображается в следующих столбцах таблицы:

- **Имя** – имя правила классификации трафика.
- **L2-поля** – L2-поля, значения которых правило классификации трафика использует для определения трафика из общего потока данных.

- **L3-поля** – L3-поля, значения которых правило классификации трафика использует для определения трафика из общего потока данных.
- **L4-поля** – L4-поля, значения которых правило классификации трафика использует для определения трафика из общего потока данных.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание правила классификации трафика

Чтобы создать правило классификации трафика:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   По умолчанию выбрана вкладка **Правила**, на которой отображается таблица правил классификации трафика.

4. В верхней части страницы нажмите на кнопку **+ Правило классификации**.

5. В открывшемся окне в поле **Имя** введите имя правила классификации трафика.

6. На вкладке **L2-поля** установите флажки рядом с L2-полями, значения которых правило классификации трафика использует для определения трафика из общего потока данных. Если флажок установлен, введите или выберите значение поля. Вы можете использовать значения следующих полей для определения трафика из общего потока данных:

   - **Внешний VLAN ID**. Диапазон значений: от 1 до 2094.
   - **Внешний VLAN PCP**. Диапазон значений: от 0 до 7.
   - **MAC источника**.
   - **Маска MAC источника**.
   - **MAC назначения**.
   - **Маска MAC назначения**.
   - **Ethertype**:
     - **0x0800**. Это значение выбрано по умолчанию.
     - **0x86dd**.
     - **0x0806**.

7. Выберите вкладку **L3-поля** и установите флажки рядом с L3-полями, значения которых правило классификации трафика использует для определения трафика из общего потока данных. Если флажок установлен, введите или выберете значение поля. Вы можете использовать значения следующих полей для определения трафика из общего потока данных.

   - **Протокол**:
     - **IPv4**.
     - **IPv6**.
   - **IP источника**.
   - **Длина префикса IP источника**. Диапазон значений для IPv4-адреса: от 0 до 32; для IPv6-адреса: от 0 до 128.
   - **IP назначения**.
   - **Длина префикса IP назначения**. Диапазон значений для IPv4-адреса: от 0 до 32; для IPv6-адреса: от 0 до 128.
   - **DSCP**.
   - **TOS**.

8. Выберите вкладку **L4-поля** и установите флажки рядом с L4-полями, значения которых правило классификации трафика использует для определения трафика из общего потока данных. Если флажок установлен, введите или выберете значение поля. Вы можете использовать значения следующих полей для определения трафика из общего потока данных:

   - **IP-протокол**.
   - **Список портов источника**.
   - **Список портов назначения**.
   - **Номер типа ICMP**.

9. Выберите вкладку **DPI**, установите флажок **Приложение** и выберите приложение, трафик которого правило классификации трафика определяет из общего потока данных.

10. Нажмите на кнопку **Создать**.

    Правило классификации трафика будет создано и отобразится в таблице.

Вы можете указать правило классификации трафика при создании или изменении фильтра трафика, чтобы фильтр трафика использовал правило классификации трафика.

Пример созданного правила классификации трафика:
Вы можете создать правило классификации трафика со следующими параметрами:

- На вкладке **L2-поля** в поле **Внешний VLAN ID** введено значение `1`.
- На вкладке **L2-поля** в поле **Внешний VLAN PCP** введено значение `3`.
- На вкладке **L3-поля** в раскрывающемся списке **Протокол** выбрано значение **IPv4**.
- На вкладке **L3-поля** в поле **IP источника** введен IP-адрес `192.168.2.0/24`.

Правило классификации трафика определяет из общего потока данных трафик со следующими характеристиками:

- Внешняя VLAN-метка – 1.
- Внешняя PCP-метка – 3.
- Протокол – IPv4.
- IP-адрес источника – 192.168.2.0/24.

Правило классификации трафика не определяет из общего потока данных трафик, у которого отсутствует хотя бы одна из этих характеристик.

Изменение правила классификации трафика

Чтобы изменить правило классификации трафика:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   По умолчанию выбрана вкладка **Правила**, на которой отображается таблица правил классификации трафика.

4. Нажмите на имя правила классификации трафика, которое вы хотите изменить, или выберите его в таблице и нажмите на кнопку **Изменить**.

5. В открывшемся окне при необходимости измените параметры правила классификации трафика. Описание параметров см. в инструкции по созданию правила классификации трафика.

6. Нажмите на кнопку **Сохранить**.

Правило классификации трафика будет изменено и обновится в таблице.

Удаление правила классификации трафика

Удаленные правила классификации трафика невозможно восстановить.

Чтобы удалить правило классификации трафика:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   По умолчанию выбрана вкладка **Правила**, на которой отображается таблица правил классификации трафика.

4. Выберите в таблице правило классификации трафика, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Правило классификации трафика будет удалено и перестанет отображаться в таблице.

Работа с фильтрами трафика

Для просмотра таблицы фильтров трафика вам нужно в меню перейти в раздел **Инфраструктура**, открыть параметры развертывания контроллера, нажав на имя контроллера или выбрав контроллер в таблице и нажав **Параметры развертывания**, затем перейти в раздел **Фильтры трафика** и выбрать вкладку **Фильтры**. Информация о фильтрах трафика отображается в следующих столбцах таблицы:

- **Имя** – имя фильтра трафика.
- **Добавленные правила** – правила классификации трафика, которые были добавлены в фильтр трафика.
- **Действие** – действие, которое фильтр трафика применяет к трафику:
  - **Разрешить** – разрешить дальнейшую маршрутизацию трафика.
  - **Запретить** – запретить дальнейшую маршрутизацию трафика.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание фильтра трафика

Чтобы создать фильтр трафика:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   По умолчанию выбрана вкладка **Правила**, на которой отображается таблица правил классификации трафика.

4. Выберите вкладку **Фильтры**.

   Отобразится таблица фильтров трафика.

5. В верхней части страницы нажмите на кнопку **+ Фильтр трафика**.

6. В открывшемся окне в поле **Имя** введите имя фильтра трафика.

7. Добавьте созданное правило классификации трафика в фильтр трафика:

   a. В поле **Порядок** введите порядковый номер правила классификации трафика. Фильтр трафика первым применяет к трафику правило классификации трафика с наименьшим значением порядкового номера. Диапазон значений: от 1 до 998. Значение по умолчанию: `10`.

      Вы не можете указать одинаковое значение порядкового номера для нескольких правил классификации трафика.

   b. В раскрывающемся списке **Правило классификации** выберите правило классификации трафика, которое вы хотите добавить в фильтр трафика.

   c. В раскрывающемся списке **Действие** выберите действие, которое фильтр трафика применяет к трафику:

      - **Разрешить** – разрешить дальнейшую маршрутизацию трафика. Это значение выбрано по умолчанию.
      - **Запретить** – запретить дальнейшую маршрутизацию трафика.

   d. Нажмите на кнопку **Добавить**.

Правило классификации трафика будет добавлено. Вы можете добавить несколько правил классификации трафика и удалить правила классификации трафика. Для удаления правила классификации трафика нажмите рядом с ним на кнопку **Удалить**.

8. В раскрывающемся списке **Действие по умолчанию** выберите действие, которое фильтр трафика применяет ко всему остальному трафику:

   - **Разрешить** – разрешить дальнейшую маршрутизацию трафика. Это значение выбрано по умолчанию.
   - **Запретить** – запретить дальнейшую маршрутизацию трафика.

9. Нажмите на кнопку **Создать**.

Фильтр трафика будет создан и отобразится в таблице.

Вы можете указать фильтр трафика при создании или изменении транспортного сервиса или ACL-интерфейса, чтобы транспортный сервис или ACL-интерфейс использовал фильтр трафика.

Изменение фильтра трафика

Чтобы изменить фильтр трафика:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   По умолчанию выбрана вкладка **Правила**, на которой отображается таблица правил классификации трафика.

4. Выберите вкладку **Фильтры**.

   Отобразится таблица фильтров трафика.

5. Нажмите на имя фильтра трафика, который вы хотите изменить, или выберите его в таблице и нажмите на кнопку **Изменить**.

6. В открывшемся окне при необходимости измените параметры фильтра трафика. Описание параметров см. в инструкции по созданию фильтра трафика.

7. Нажмите на кнопку **Сохранить**.

Фильтр трафика будет изменен и обновится в таблице.

Удаление фильтра трафика

Удаленные фильтры трафика невозможно восстановить.

Чтобы удалить фильтр трафика:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   По умолчанию выбрана вкладка **Правила**, на которой отображается таблица правил классификации трафика.

4. Выберите вкладку **Фильтры**.

   Отобразится таблица фильтров трафика.

5. Выберите в таблице фильтр трафика, который вы хотите удалить, и нажмите на кнопку **Удалить**.

6. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Фильтр трафика будет удален и перестанет отображаться в таблице.

Передача трафика между устройствами CPE и клиентскими устройствами с помощью транспортных сервисов

О транспортных сервисах

Вы можете использовать *транспортные сервисы* для передачи трафика между устройствами CPE и подключенными к ним клиентскими устройствами. Транспортные сервисы строятся поверх сегментов и состоят из сервисных интерфейсов. Kaspersky SD-WAN поддерживает создание следующих транспортных сервисов:

- L2:
  - Point-to-Point (E-line в классификации MEF, далее также P2P-сервис) – статический транспортный сервис, в рамках которого трафик передается между двумя сервисными интерфейсами.
  - Point-to-Multipoint (E-tree в классификации MEF, далее также P2M-сервис) – транспортный сервис, в рамках которого трафик передается между несколькими сервисными интерфейсами в соответствии с топологией дерево. Вам нужно назначить каждому добавленному в P2M-сервис сервисному интерфейсу одну из следующих ролей:
    - **Root** – сервисный интерфейс может передавать трафик на сервисный интерфейс с любой ролью.
    - **Leaf** – сервисный интерфейс может передавать трафик только на сервисные интерфейсы с ролью **Root**.
  - Multipoint-to-Multipoint (E-LAN в классификации MEF, далее также M2M-сервис) – транспортный сервис, в рамках которого трафик передается между несколькими сервисными интерфейсами без иерархии.

  P2P-сервис является статическим транспортным сервисом и не использует механизм изучения MAC-адресов (англ. MAC learning) для заполнения MAC-таблицы на контроллере. MAC-адреса автоматически добавляются в MAC-таблицу на контроллере при создании или изменении P2P-сервиса. Механизм изучения MAC-адресов используется для P2M-сервисов и M2M-сервисов.
- IP multicast (далее также IP multicast-сервис) – транспортный сервис, в рамках которого строится дерево распространения multicast-трафика между несколькими сервисными интерфейсами.
- L3 VPN (далее также L3 VPN-сервис) – транспортный сервис, в рамках которого трафик маршрутизируется между несколькими L3-интерфейсами, которые ссылаются на сервисные интерфейсы или M2M-сервисы.

При создании или изменении транспортных сервисов вы можете добавлять резервные сервисные интерфейсы. Использование резервного сервисного интерфейса позволяет продолжать передачу данных в случае выхода из строя основного сервисного интерфейса. Резервные и основные сервисные интерфейсы могут быть созданы на одном или разных устройствах CPE.

Трафик можно зеркалировать или перенаправлять между сервисными интерфейсами устройств CPE. При этом сервисные интерфейсы могут быть добавлены в транспортный сервис.

Работа с транспортными сервисами в шаблоне экземпляра SD-WAN и шаблоне CPE

Вы можете создать P2M-сервисы и M2M-сервисы, а также L3 VPN-сервисы в шаблоне экземпляра SD-WAN, после чего использовать его при развертывании экземпляра SD-WAN. Созданные в шаблоне экземпляра SD-WAN транспортные сервисы автоматически создаются для развернутого экземпляра SD-WAN. Это позволяет создавать транспортные сервисы до развертывания экземпляра SD-WAN.

Созданные для развернутого экземпляра SD-WAN транспортные сервисы можно добавить в шаблон CPE, после чего указать его при добавлении или ручной регистрации устройств CPE. В этом случае автоматически создаются сервисные интерфейсы, ссылающиеся на OpenFlow-порты, на которые ссылаются интерфейсы SD-WAN с типом LAN устройств CPE. Автоматически созданные сервисные интерфейсы добавляются в транспортные сервисы, которые вы добавили в шаблон CPE. Это позволяет не подключать вручную каждое устройство CPE к транспортным сервисам.

Управляющий транспортный сервис

При регистрации устройства CPE автоматически подключаются к управляющему транспортному сервису. Через управляющий транспортный сервис передается трафик SSH-консоли, запускаются скрипты и передаются API-команды для управления VIM, развернутым на устройстве uCPE.

В каждом шаблоне экземпляра SD-WAN по умолчанию создан управляющий транспортный сервис P2M. При создании или изменении P2M-сервиса или M2M-сервиса в шаблоне экземпляра SD-WAN вы можете сделать P2M-сервис или M2M-сервис управляющим сервисом.

При необходимости через управляющий транспортный сервис можно передавать трафик мониторинга Zabbix, а также трафик протоколов syslog и NetFlow. Трафик мониторинга Zabbix зашифрован по умолчанию, в то время как для шифровки трафика протоколов syslog и NetFlow трафик необходимо передавать через управляющий транспортный сервис. Передача трафика протоколов syslog и NetFlow через управляющий транспортный сервис определяется параметрами таблицы маршрутизации устройств CPE.

Дублирование пакетов трафика

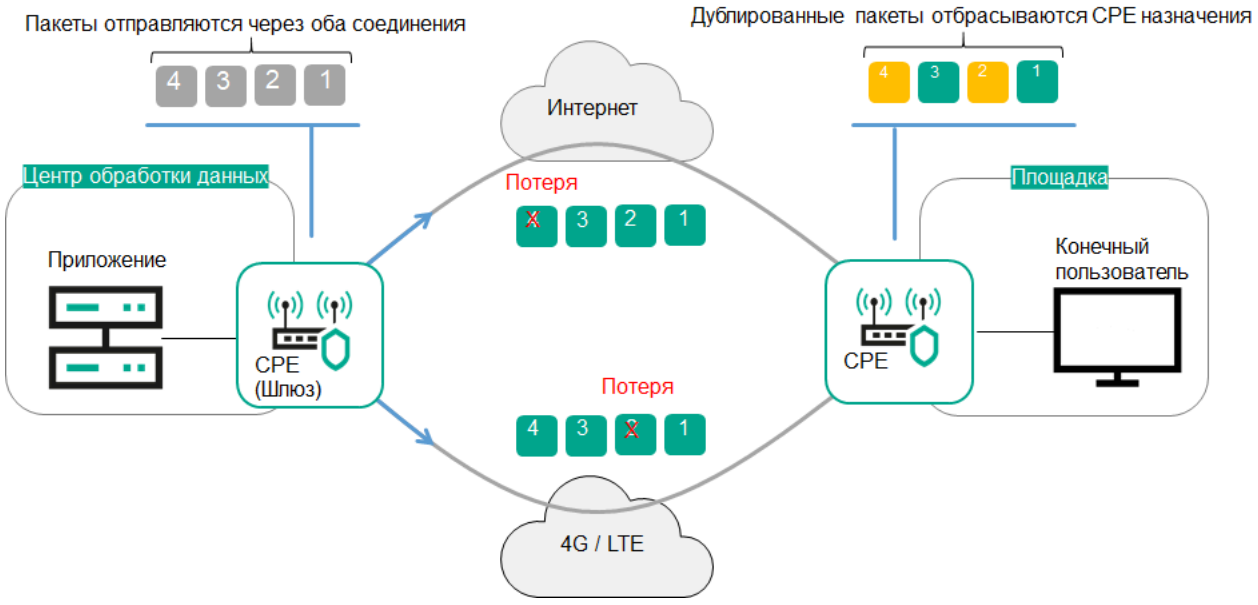
Вы можете включить дублирование пакетов трафика для предотвращения потерь при передаче пакетов трафика через следующие транспортные сервисы:

- P2P-сервисы.
- P2M-сервисы.
- M2M-сервисы.
- L3 VPN-сервисы.
- TAP-сервисы.

Если дублирование пакетов трафика включено для транспортного сервиса, устройство CPE источника дублирует пакеты трафика и передает их через все соединения. Устройство CPE назначения получает пакеты трафика и отбрасывает лишние пакеты трафика. Если пакет трафика утрачивается при передаче через соединение, устройство CPE назначения может получить пакет трафика через другое соединение. Дублирование пакетов трафика можно использовать для приложений, которые пользуются большим спросом, такие как банкоматы и POS-терминалы.

Для включения дублирования пакетов трафика вам нужно выбрать значение **Широковещательный** в раскрывающемся списке **Режим балансировки** при создании или изменении транспортного сервиса.

Например, на рисунке ниже изображено устройство CPE с ролью шлюза в центре обработки данных, которое передает через два соединения пакеты трафика приложения стандартному устройству CPE на удаленной площадке. Стандартное устройство CPE на удаленной площадке в свою очередь передает пакеты трафика конечным пользователям. Оба устройства CPE добавлены в транспортный сервис, для которого включено дублирование пакетов трафика, поэтому пакеты трафика дублируются и передаются одновременно через два соединения.



Дублирование пакетов трафика между устройствами CPE

Сценарий: направление трафика приложения в транспортный сервис

Сценарий направления трафика приложения в транспортный сервис состоит из следующих этапов:

1. **Создание транспортного сервиса**

   Создайте транспортный сервис, в который вы хотите направлять трафик приложения. Для выполнения этого этапа вы можете использовать следующие инструкции:

   - Создание P2P-сервиса.
   - Создание P2M-сервиса.
   - Создание M2M-сервиса.
   - Создание IP multicast-сервиса.
   - Создание L3 VPN-сервиса.

2. **Создание правила классификации трафика**

   Создайте правило классификации трафика для определения трафика приложения из общего потока данных. При создании правила классификации трафика вам нужно выбрать протокол уровня L3 на вкладке **L3-поля**, а также приложение, трафик которого вы хотите направить в транспортный сервис, на вкладке **DPI**.

Если вы хотите направить в транспортный сервис трафик нескольких приложений, вам нужно создать отдельное правило классификации трафика для каждого приложения.

3. **Создание фильтра трафика**

   Создайте фильтр трафика, чтобы определить, разрешена ли маршрутизация трафика приложения. При создании фильтра трафика вам нужно добавить в него правила классификации трафика, которые вы создали для трафика приложения.

4. **Создание ACL-интерфейса**

   Создайте ACL-интерфейс, чтобы применять фильтр трафика к трафику, который передается через ACL-интерфейс. При создании ACL-интерфейса вам нужно выбрать фильтр трафика, который вы создали для трафика приложения.

5. **Добавление ACL-интерфейса в транспортный сервис**

   Измените транспортный сервис и добавьте в него ACL-интерфейс, который вы создали для трафика приложения. Для выполнения этого этапа вы можете использовать следующие инструкции:

   - Изменение P2P-сервиса.
   - Изменение P2M-сервиса.
   - Изменение M2M-сервиса.
   - Изменение IP multicast-сервиса.
   - Изменение L3 VPN-сервиса.

Трафик приложения будет направляться в транспортный сервис.

Сценарий: обеспечение L2-связности между устройствами CPE

Вы можете обеспечить L2-связность между устройствами CPE для выполнения следующих задач:

- Создание L2-домена, в который входят несколько удаленных площадок.
- Передача L2-трафика для keepalive-соединений между устройствами CPE, установленными на разных удаленных площадках.
- Осуществление пользовательских сценариев зеркалирования трафика.

Сценарий обеспечения L2-связности между устройствами CPE состоит из следующих этапов:

1 **Создание OpenFlow-портов на виртуальных коммутаторах устройств CPE**

1. При создании или изменении сетевого интерфейса без IP-адреса на устройствах CPE, между которыми вы хотите обеспечить L2-связность, установите флажок **L2-режим**. Когда флажок установлен, на виртуальном коммутаторе устройства CPE автоматически создается OpenFlow-порт, ссылающийся на сетевой интерфейс. Этот флажок снят по умолчанию. Вы не можете установить флажок в следующих случаях:

   - При создании сетевого интерфейса вы установили следующие флажки:
     - **Мост**.
     - **NetFlow**.
     - **Назначать IP, маршрут и шлюз**.
   - Сетевой интерфейс используется в статическом маршруте.
   - Сетевой интерфейс используется протоколом BGP.
   - Сетевой интерфейс используется протоколом OSPF.
   - Сетевой интерфейс используется протоколом VRRP.
   - Сетевой интерфейс используется для передачи multicast-трафика.
   - Сетевой интерфейс используется виртуальной таблицей маршрутизации (VRF).
   - Сетевой интерфейс используется для диагностики устройства CPE с помощью утилиты ping, traceroute, tcpdump и/или sweep.

   Номер OpenFlow-порта, который автоматически создается на виртуальном коммутаторе устройства CPE, отобразится в поле **OpenFlow-порт**. Вы можете изменить номер OpenFlow-порта. Диапазон значений: от 11 до 20.

1 **Создание сервисных интерфейсов, ссылающихся на OpenFlow-порты**

Создайте сервисные интерфейсы, ссылающиеся на OpenFlow-порты, автоматически созданные на предыдущем этапе этого сценария. Вам нужно выбрать OpenFlow-порт, на который ссылается сервисный интерфейс, в раскрывающемся списке **Порт**.

2 **Добавление сервисных интерфейсов в транспортный сервис**

Добавьте сервисные интерфейсы, созданные на предыдущем этапе этого сценария, в транспортный сервис, с помощью которого вы хотите обеспечить L2-связность между устройствами CPE. Для выполнения этого этапа вы можете использовать следующие инструкции:

- Создание P2P-сервиса и Изменение P2P-сервиса.
- Создание P2M-сервиса и Изменение P2M-сервиса.
- Создание M2M-сервиса и Изменение M2M-сервиса.
- Создание L3 VPN-сервиса и Изменение L3 VPN-сервиса.
- Создание IP multicast-сервиса и Изменение IP multicast-сервиса.
- Создание TAP-сервиса и Изменение TAP-сервиса.

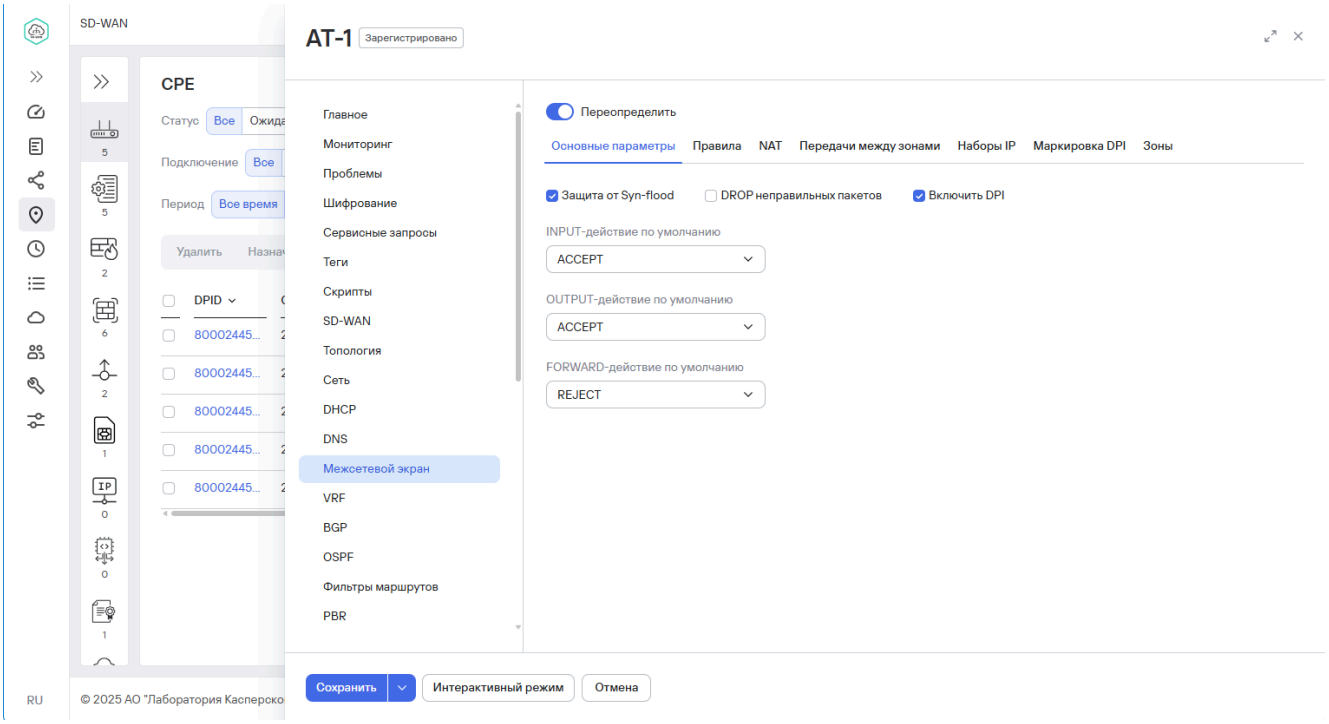
Между устройствами CPE будет обеспечена L2-связность.

Сценарий: управление трафиком приложений в соответствии с заданным SLA

Сценарий управления трафиком приложения в соответствии с заданным SLA состоит из следующих этапов:

1. **Включение DPI (Deep Packet Inspection, глубокий анализ пакетов) глобально в настройках межсетевого экрана**

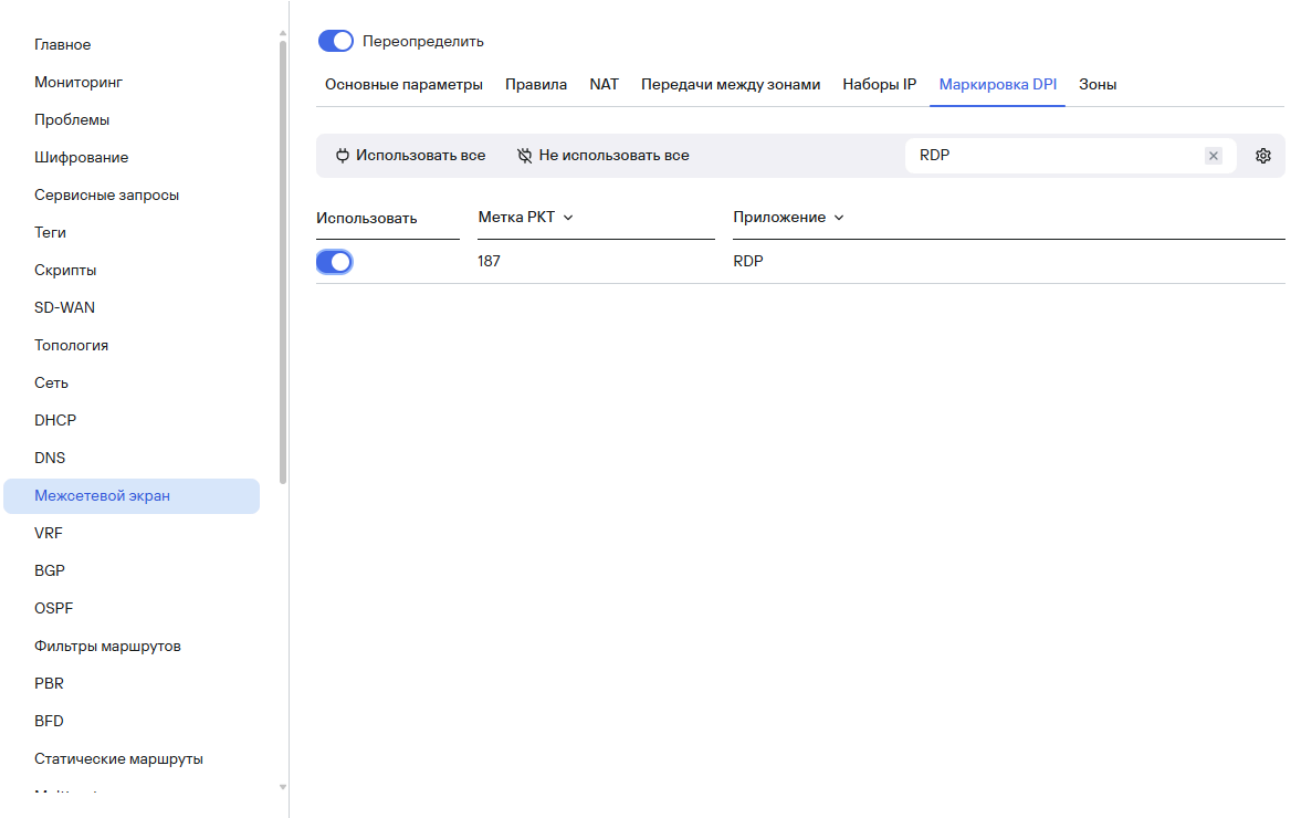
   Убедитесь, что в области настройки основных параметров межсетевого экрана на устройстве CPE или в шаблоне межсетевого экрана установлен флажок **Включить DPI**:



Окно настроек CPE. Включение функции DPI.

2. **Включение распознавания приложений с помощью DPI для RDP**

В области настройки параметров межсетевого экрана устройства CPE или шаблона межсетевого экрана перейдите во вкладку **Маркировка DPI**, найдите в таблице и приложение **RDP** и включите для него переключатель **Использовать**:

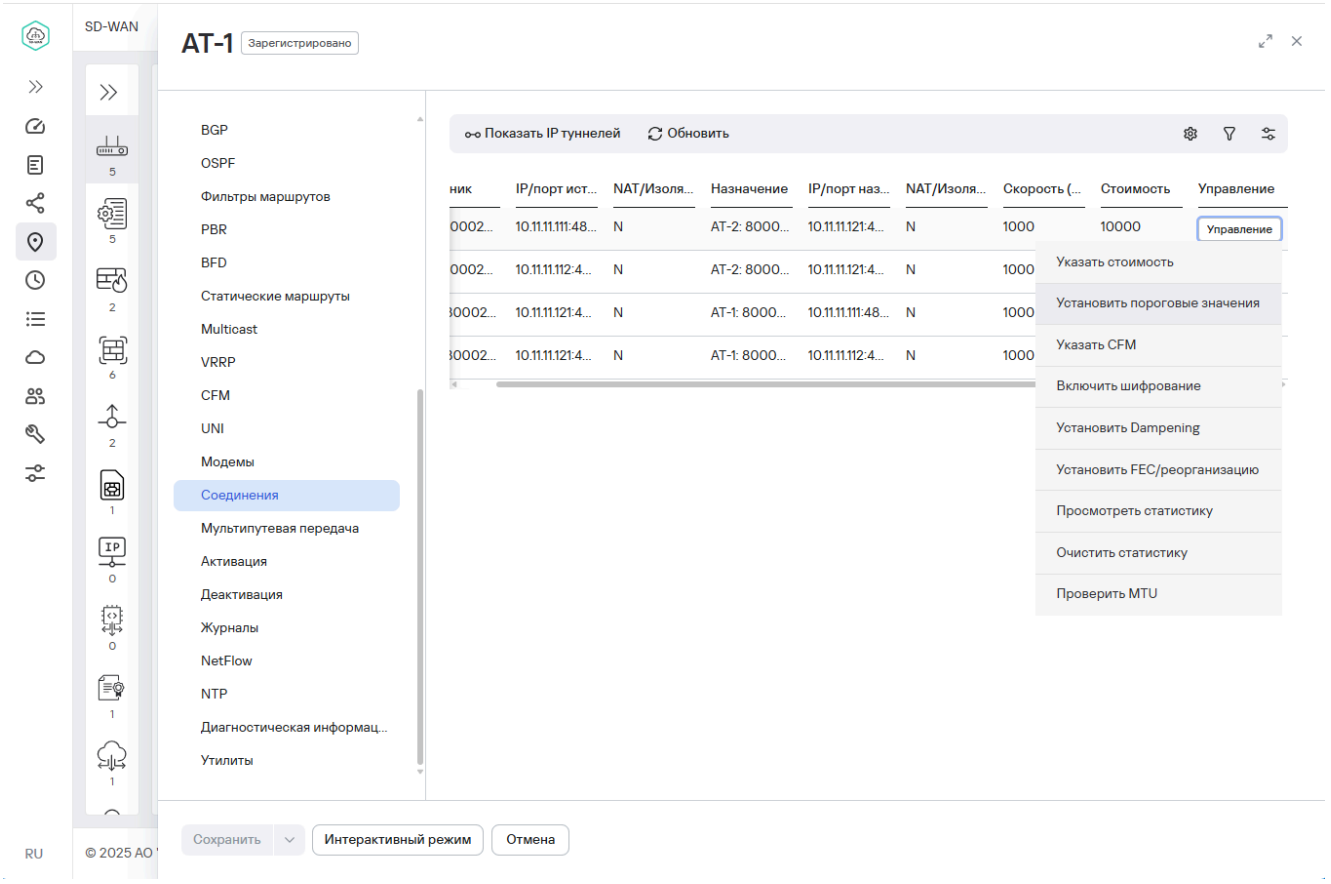


Включение DPI для распознавания RDP

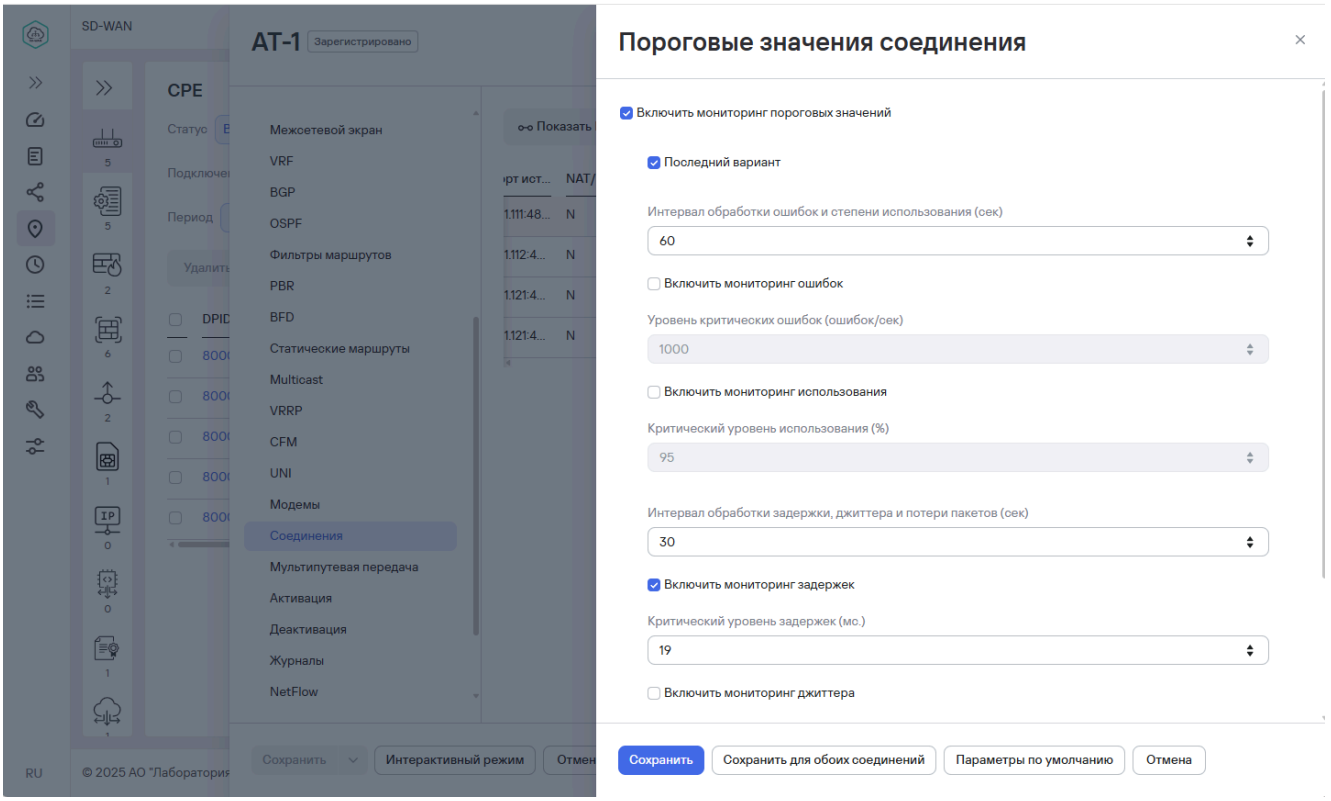
Более подробно о настройке DPI см. в статье Настройка маркировки DPI.

3 Включение мониторинга трафика на соединениях CPE

Используя инструкцию Мониторинг соединения, на нужном соединении устройства CPE включите мониторинг пороговых значений, установите флажок Последний вариант, и для параметра Критический уровень задержек (мс) укажите значение, незначительно превышающее задержки на выбранном соединении:



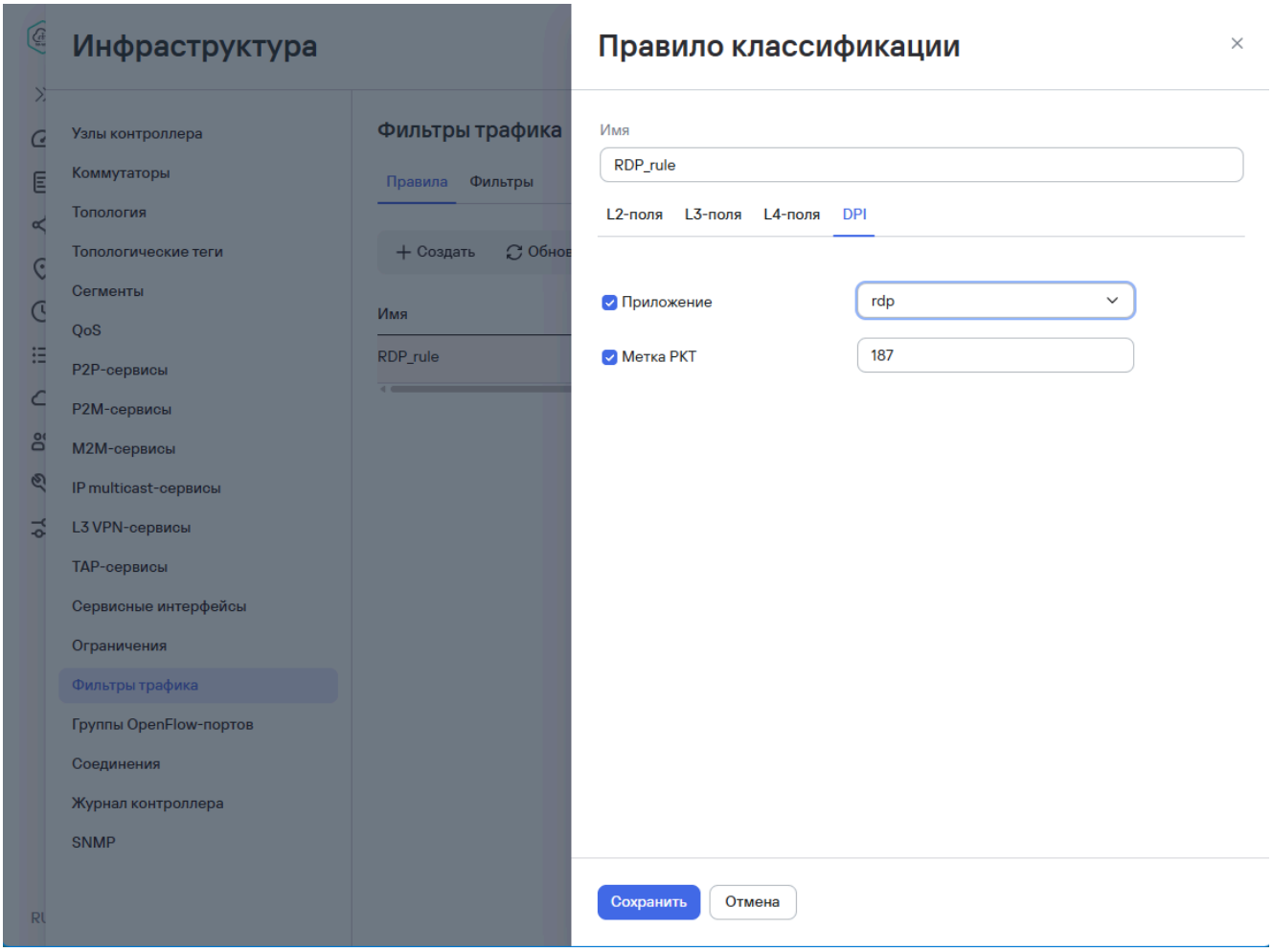
Переход к созданию пороговых значений на соединении устройства CPE



Включение мониторинга задержек к указанием критического уровня задержек

4 Создание правила классификации трафика приложения

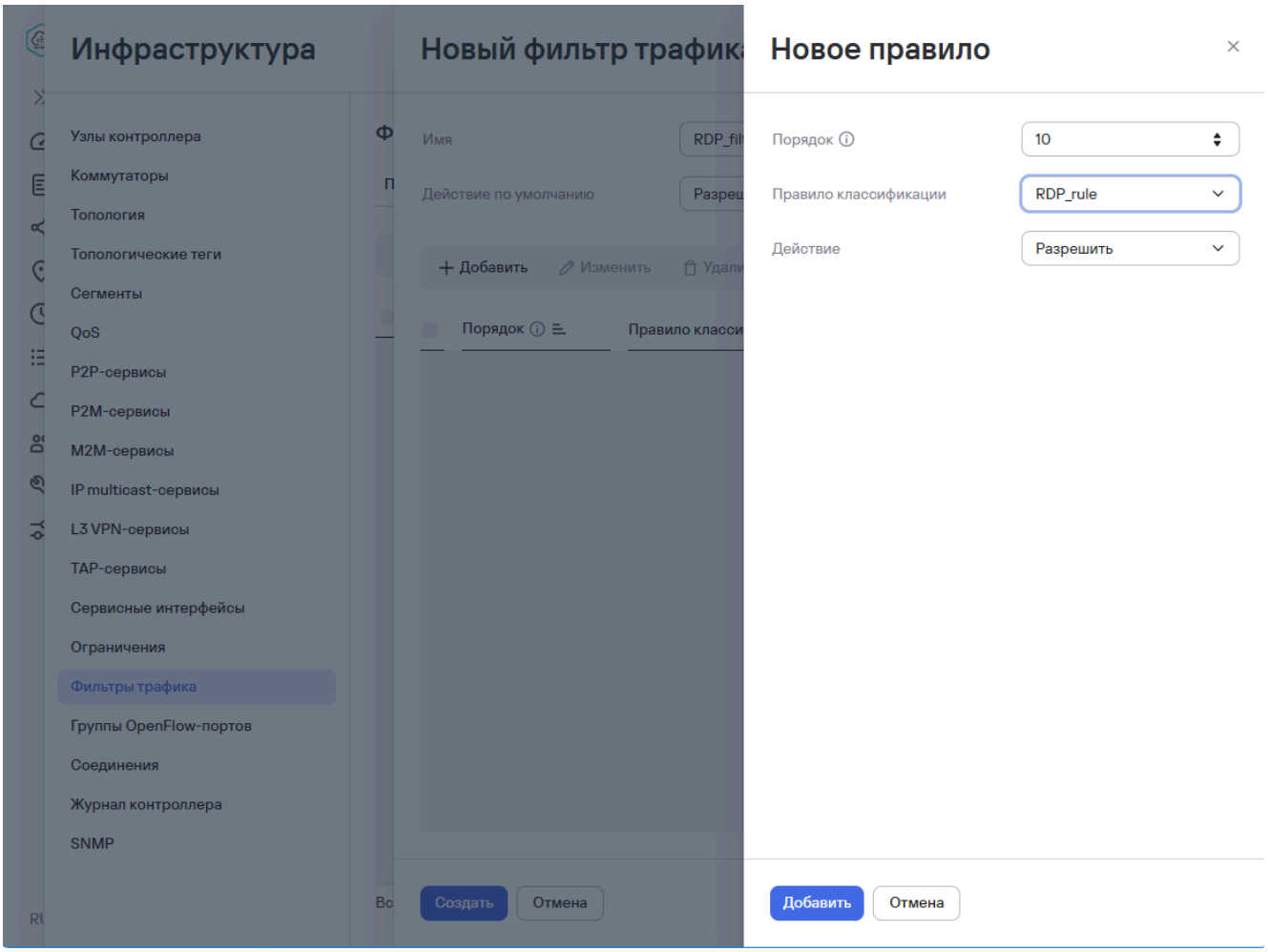
Создайте правило классификации трафика, указав на вкладке **DPI** для классификации приложения значение **dpi**:



Создание правила классификации трафика для приложения RDP

5 Создание фильтра для выделения трафика приложения

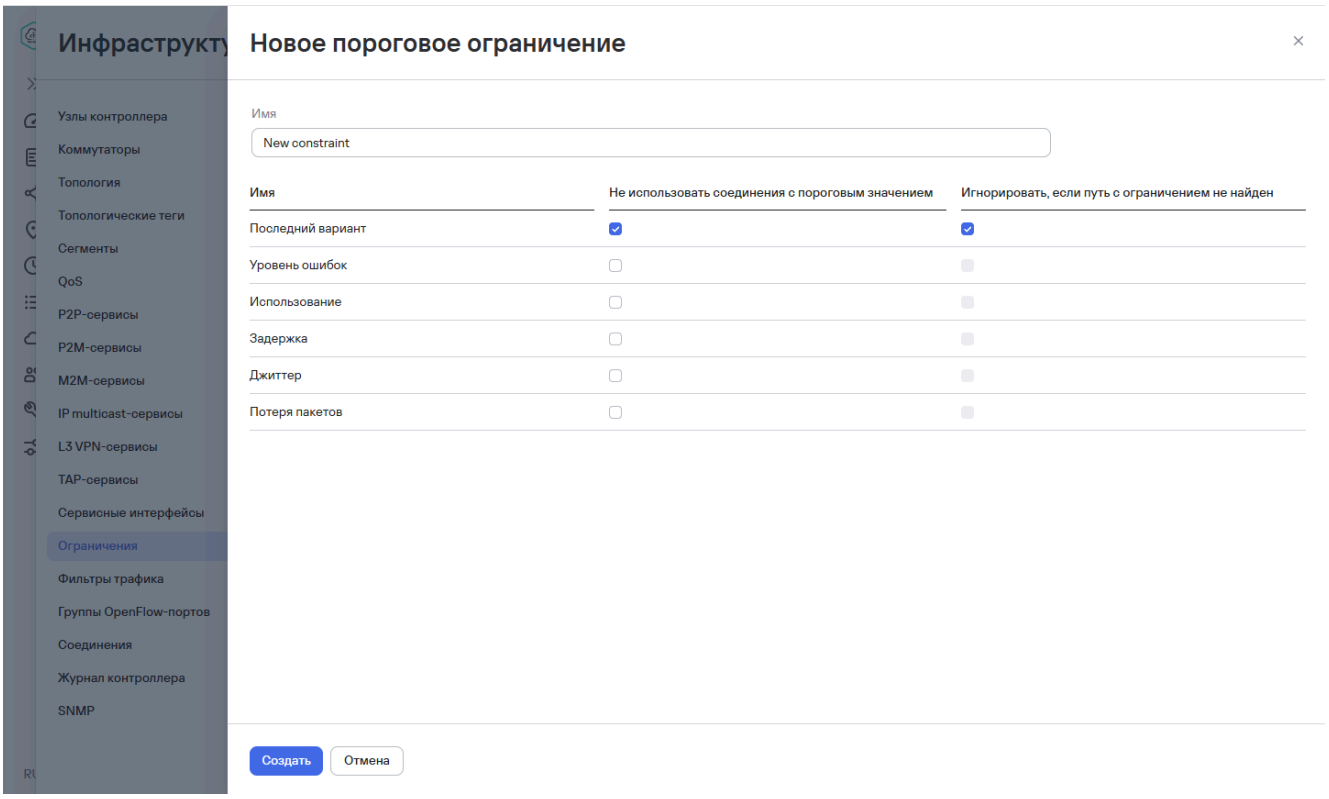
Создайте фильтр трафика и добавьте в него правило классификации, созданное на предыдущем шаге:



Создание фильтра трафика

6 Создание пороговых ограничений

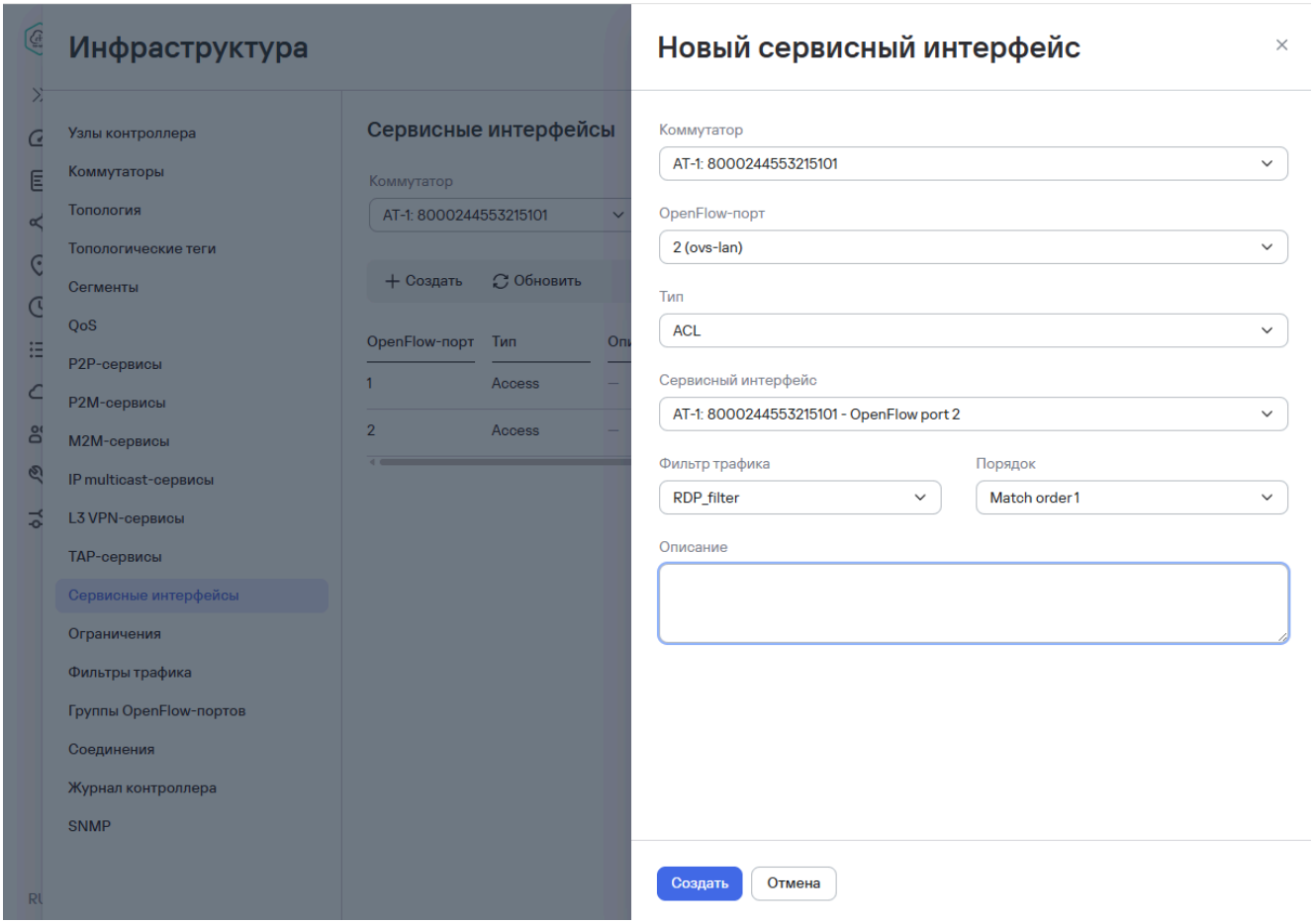
Создайте пороговое ограничение для контроллера, выберите в качестве показателя мониторинга **Последний вариант** и установите для него оба флажка **Не использовать соединения с пороговым значением** и **Игнорировать, если путь с ограничением не найден**:



Создание порогового значения с показателем мониторинга "Последний вариант"

7 Создание сервисных интерфейсов ACL

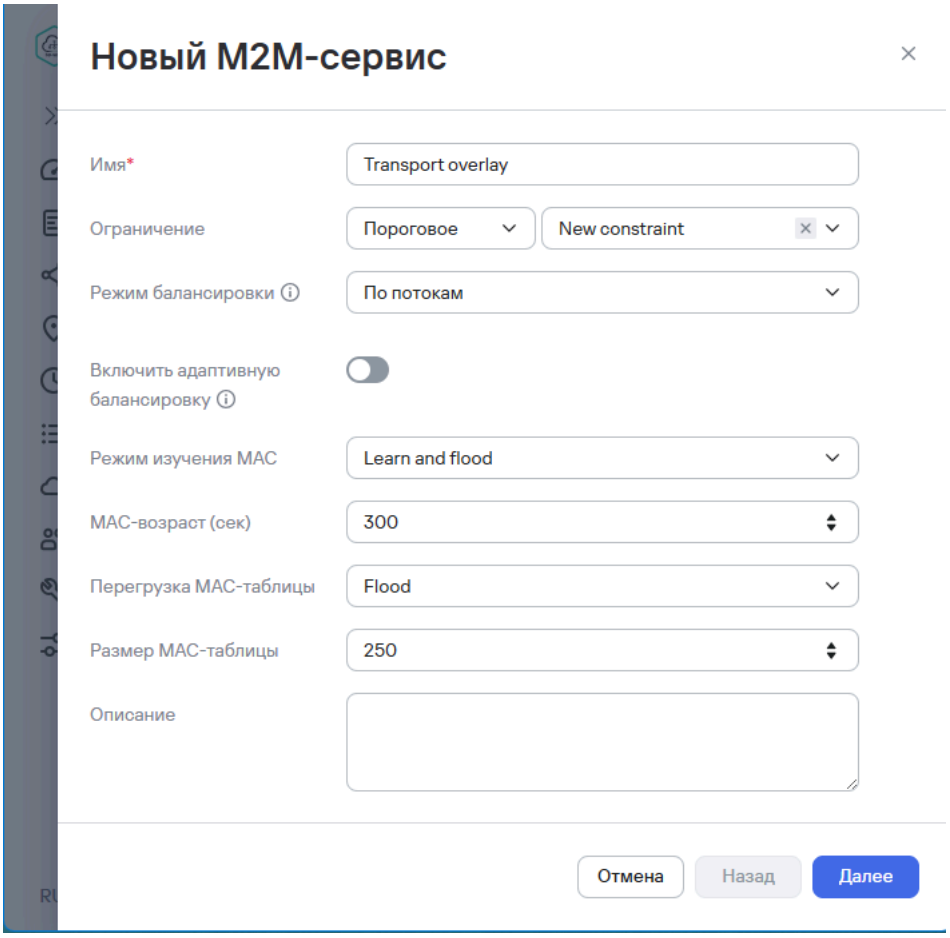
Создайте сервисные интерфейсы с типом ACL для CPE с ролью шлюза и стандартного CPE. При создании укажите сервисный интерфейс основного M2M-сервиса и ранее созданный фильтр для трафика RDP:



Добавление ACL-интерфейса с ранее созданным фильтром трафика

8 Создание отдельного M2M-сервиса

Создайте M2M-сервис, в который будет попадать только трафик RDP. Включите в этот сервис только ACL-интерфейсы, созданные на предыдущем шаге, и укажите созданное ранее пороговое ограничение New constraint:



Добавление M2M-сервиса с пороговым ограничением

Трафик RDP будет попадать в новый M2M-сервис. Остальной трафик будет попадать в основной сервисный интерфейс и распределяться между доступными соединениями.

Работа с транспортными сервисами Point-to-Point (P2P)

Для просмотра таблицы P2P-сервисов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **P2P-сервисы**. Информация о P2P-сервисах отображается в следующих столбцах таблицы:

- **Имя** – имя P2P-сервиса.
- **Источник** – информация о сервисном интерфейсе источника P2P-сервиса:
  - имя и идентификатор DPID устройства CPE, на котором создан сервисный интерфейс;
  - номер OpenFlow-порта, на который ссылается сервисный интерфейс.

- **Назначение** – информация о сервисном интерфейсе назначения P2P-сервиса:
  - имя и идентификатор DPID устройства CPE, на котором создан сервисный интерфейс;
  - номер OpenFlow-порта, на который ссылается сервисный интерфейс.
- **QoS** – правило качества обслуживания, указанное для сервисного интерфейса источника P2P-сервиса.
- **Резервный сервисный интерфейс** – информация о резервном сервисном интерфейсе источника P2P-сервиса:
  - имя и идентификатор DPID устройства CPE, на котором создан сервисный интерфейс;
  - номер OpenFlow-порта, на который ссылается сервисный интерфейс.
- **Статус** – статус P2P-сервиса:
  - **Работает**.
  - **Не работает**.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание P2P-сервиса

Чтобы создать P2P-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2P-сервисы**.

   Отобразится таблица P2P-сервисов.

4. В верхней части страницы нажмите на кнопку **+ P2P-сервис**.

5. В открывшемся окне в поле **Имя** введите имя P2P-сервиса.

6. В раскрывающемся списке **Ограничение** выберите созданное ограничение Manual-TE или пороговое ограничение, которое вы хотите добавить в P2P-сервис.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для распределения трафика по соединениям:

   - **По потокам** – потоки трафика (5-Tuple) распределяются по соединениям в соответствии со стоимостью соединений. Это значение выбрано по умолчанию.
   - **По пакетам** – пакеты трафика распределяются по соединениям в соответствии со стоимостью соединений.
   - **Широковещательный** – пакеты трафика дублируются и передаются одновременно через все соединения для исключения потерь.

   Вы можете указать стоимость соединения вручную.

8. При необходимости настройте режим адаптивной балансировки, если хотите, чтобы вес пути динамически корректировался в зависимости от уровня пакетных потерь на пути:

   a. Включите переключатель **Включить адаптивную балансировку**.

   b. В поле **Минимальный уровень потерь (%)** укажите минимальный процент пакетных потерь на пути, при котором режим адаптивной балансировки начинает влиять на вес. Диапазон значений: 0.01 – 100.

   c. В поле **Максимальный уровень потерь (%)** укажите максимальный процент пакетных потерь, при котором путь исключается из балансировки нагрузки.

   d. В раскрывающемся списке **Скорость схождения** выберите скорость схождения адаптивных весов к расчетным значениям:

      - **Fast** – 1;
      - **Fast** – 0,75;
      - **Fast** – 0,5.

9. При необходимости в поле **Описание** введите краткое описание P2P-сервиса.

10. В раскрывающихся списках **Коммутатор** и **Сервисный интерфейс** слева выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как сервисный интерфейс источника P2P-сервиса.

11. В раскрывающихся списках **Коммутатор** и **Сервисный интерфейс** справа выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как сервисный интерфейс назначения P2P-сервиса.

12. Если вы хотите отобразить в раскрывающихся списках **Сервисный интерфейс** сервисные интерфейсы, которые добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. Этот флажок снят по умолчанию.

13. Если вы хотите поменять местами значения, выбранные в раскрывающихся списках **Сервисный интерфейс**, установите флажок **Переключить интерфейсы**. Этот флажок снят по умолчанию.

14. Если вы хотите добавить резервный сервисный интерфейс источника P2P-сервиса, через который трафик передается при выходе из строя основного сервисного интерфейса, выполните следующие действия:

    a. Установите флажок **Резервный интерфейс**. Этот флажок снят по умолчанию.

    b. В раскрывающихся списках **Резервный коммутатор** и **Резервный сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как резервный сервисный интерфейс.

    c. Если вы хотите отобразить в раскрывающемся списке **Резервный сервисный интерфейс** сервисные интерфейсы, которые добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. Этот флажок снят по умолчанию.

    Если основной сервисный интерфейс источника P2P-сервиса возобновляет работу, P2P-сервис продолжает использовать резервный сервисный интерфейс источника.

15. В раскрывающихся списках **Входящий фильтр** слева и справа выберите созданный фильтр трафика для сервисных интерфейсов источника и назначения P2P-сервиса.

16. В раскрывающемся списке **QoS** выберите созданное правило качества обслуживания для сервисного интерфейса источника P2P-сервиса.

17. Если вы хотите отслеживать состояние сервисных интерфейсов источника и назначения P2P-сервиса и при выключении одного сервисного интерфейса автоматически выключать второй, установите флажок **Транслировать статус интерфейса**. Этот флажок снят по умолчанию. Флажок невозможно установить, если установлен флажок **Резервный интерфейс**.

    Когда сервисный интерфейс, который был выключен первым, восстанавливает работу, второй автоматически выключенный сервисный интерфейс также восстанавливает работу. Эта функция работает только на сервисных интерфейсах с классификацией трафика Access. Вы можете выбрать тип классификации трафика при создании сервисного интерфейса.

18. Нажмите на кнопку **Создать**.

P2P-сервис будет создан и отобразится в таблице.

Просмотр статистики работы P2P-сервиса

Чтобы посмотреть статистику работы P2P-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2P-сервисы**.

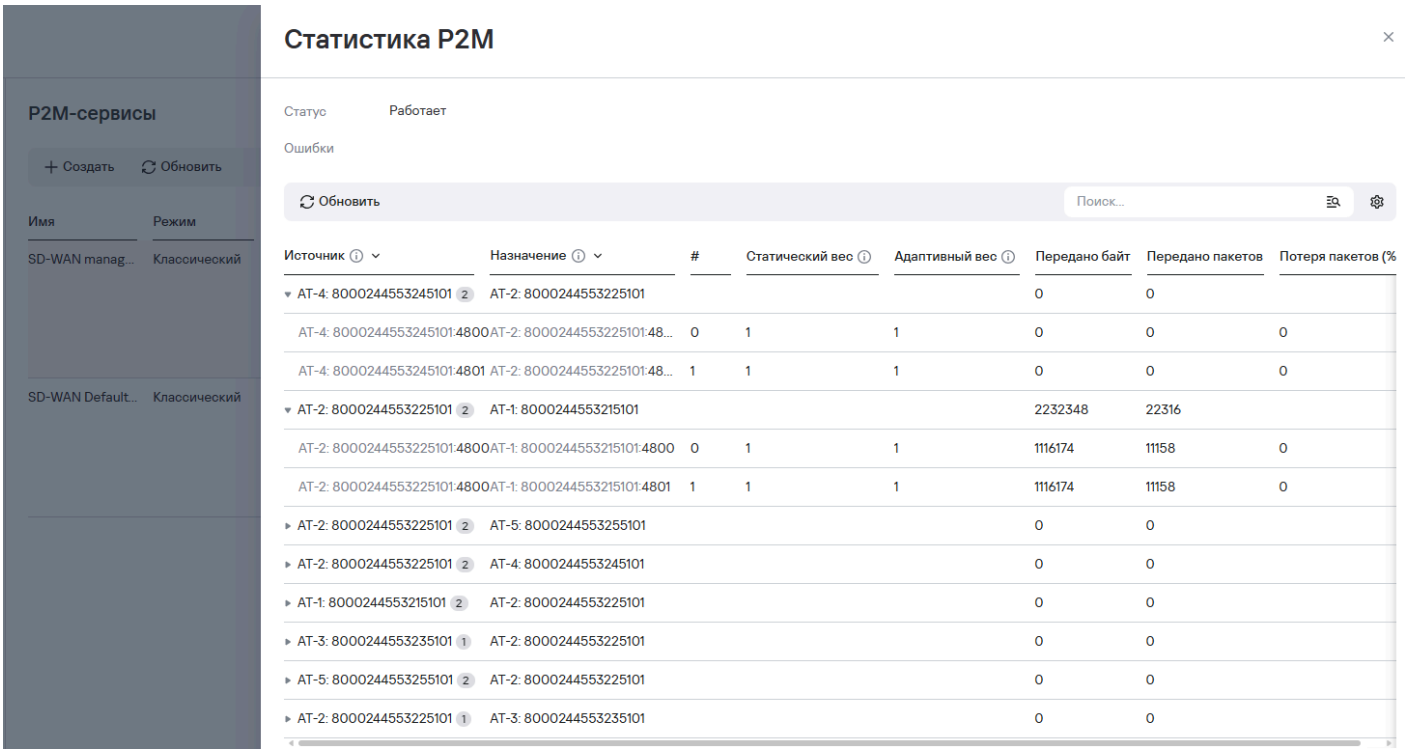
   Отобразится таблица P2P-сервисов.

4. Нажмите на кнопку **Управление** → **Статистика** рядом с P2P-сервисом, статистику работы которого вы хотите посмотреть.

Откроется окно со статистикой работы P2P-сервиса.

В верхней части окна статистики в поле **Статус** отображается операционный статус сервиса. В поле **Ошибки** показываются возможные ошибки, возникающие на сервисе.

Статистика по сегментам, путям и соединениям сервиса отображается в таблице в иерархическом виде. Строки в таблице сгруппированы по сегментам. Строки внутри каждой группы содержат статистику по путям, входящим в соответствующий сегмент. Группу можно раскрыть, нажав на треугольник (▸). У сервисов, для которых не заданы ограничения, в строках отображаются все пути с включенной в сегменте балансировкой нагрузки. У сервисов, для которых заданы ограничения, в строках отображаются пути Auto-TE, удовлетворяющие ограничению.



Отображение статистики на примере P2M-сервиса

Подробная информация статистики о сегментах и путях отображается в следующих столбцах таблицы:

Источник – для агрегирующих строк: исходный узел сегмента, для строк в раскрывающихся группах: исходный узел пути в сегменте.

Назначение – для агрегирующих строк: конечный узел сегмента, для строк в раскрывающихся группах: конечный узел пути в сегменте.

– порядковый номер пути. Чем меньше порядковый номер пути, тем раньше путь был построен. Значение отображается только у строк в раскрывающихся группах.

Статический вес – статический вес пути на основе стоимости. Значение отображается только у строк в раскрывающихся группах.

Адаптивный вес – динамический вес пути на основе анализа потерь пакетов на данном пути. Значение отображается только у строк в раскрывающихся группах. Если механизм адаптивной балансировки не используется, столбец не отображается.

Передано байт – для агрегирующих строк: значение из текущего окна статистики сервиса, для строк в раскрывающихся группах: количество переданных в бакет OF-группы байтов.

Передано пакетов – для агрегирующих строк: значение из текущего окна статистики сервиса, для строк в раскрывающихся группах: количество переданных в бакет OF-группы пакетов.

Потеря пакетов (%) – процентная потеря пакетов на данном пути (отношение количества потерянных пакетов к общему количеству отправленных пакетов). Значение отображается только у строк в раскрывающихся группах.

Просмотр и настройка отображения топологии P2P-сервиса

Чтобы посмотреть и настроить отображение топологии P2P-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2P-сервисы**.

   Отобразится таблица P2P-сервисов.

4. Нажмите на кнопку **Управление** → **Топология сервиса** рядом с P2P-сервисом, топологию которого вы хотите посмотреть.

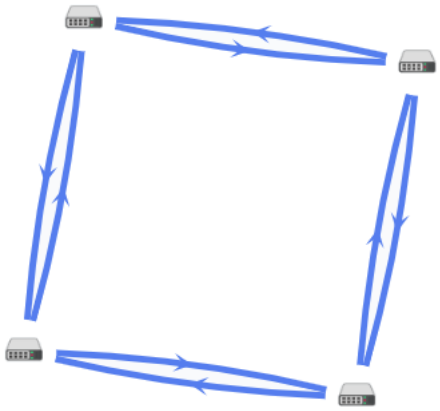
   Откроется окно с топологией P2P-сервиса.

5. При необходимости изменить расположение устройств CPE выполните одно из следующих действий:

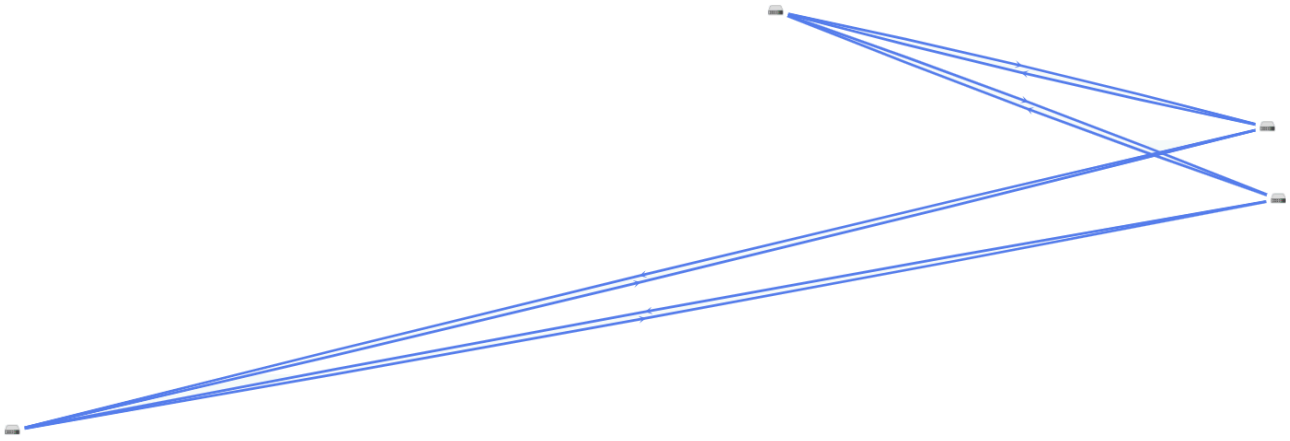
- Если вы хотите вручную изменить расположение устройств CPE, нажмите на кнопку **Вручную** и измените расположение устройств CPE.

- Если вы хотите автоматически расположить устройства CPE, нажмите на кнопку **Автоматически** и выберите одно из следующих значений в отобразившемся раскрывающемся списке:

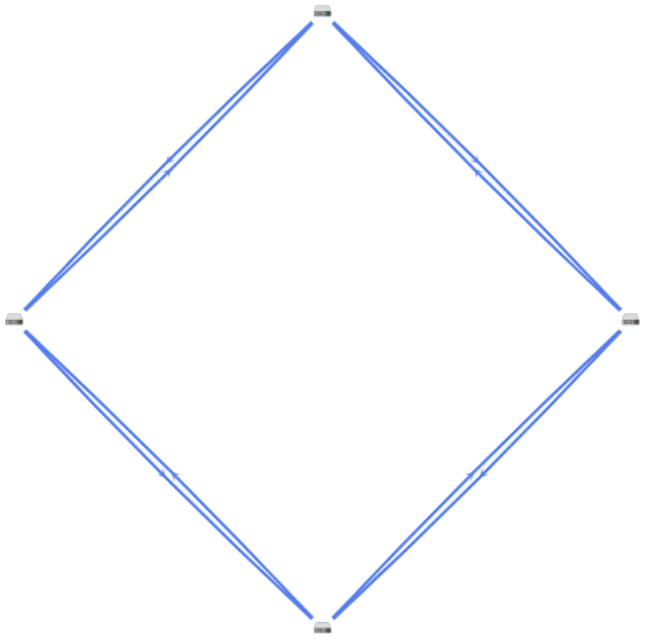
  - **Физическая симуляция** – устройства CPE располагаются примерно в соответствии с их реальным расположением относительно друг друга, например:



  - **Случайно** – устройства CPE располагаются случайным образом, например:

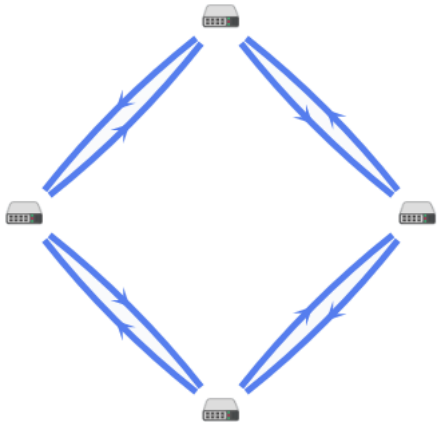


  - **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо, например:



- **Горизонтально** – устройства CPE располагаются горизонтально (в ширину), например:

- **Концентрически** – устройства CPE располагаются концентрически, например:



- **Решетка** – устройства CPE располагаются в соответствии с топологией решетка, например:

6. Если вы хотите отобразить информацию об устройствах CPE, установите следующие флажки:

   - **Имя** – отобразить имена устройств CPE.
   - **IP-адрес** – отобразить IP-адреса устройств CPE.

   По умолчанию флажки сняты.

7. Если вы хотите отобразить сегмент между двумя устройствами CPE, выполните следующие действия:

   a. Установите флажок **Сегменты**. Этот флажок снят по умолчанию.

   b. В отобразившихся раскрывающихся списках выберите устройство CPE источника и назначения сегмента.

   Отобразится сегмент между устройствами CPE.

Изменение P2P-сервиса

Чтобы изменить P2P-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2P-сервисы**.

   Отобразится таблица P2P-сервисов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с P2P-сервисом, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры P2P-сервиса. Описание параметров см. в инструкции по созданию P2P-сервиса.

6. Нажмите на кнопку **Сохранить**.

P2P-сервис будет изменен и обновится в таблице.

Перезагрузка P2P-сервиса

Вы можете перезагрузить P2P-сервис, чтобы восстановить его работу при возникновении неполадок. Когда вы перезагружаете P2P-сервис, контроллер автоматически удаляет и повторно создает связанные с P2P-сервисом правила в OpenFlow-таблицах устройств CPE. Это затрагивает устройства CPE, сервисные интерфейсы которых добавлены в P2P-сервис.

Чтобы перезагрузить P2P-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2P-сервисы**.

   Отобразится таблица P2P-сервисов.

4. Нажмите на кнопку **Управление** → **Перезагрузить** рядом с P2P-сервисом, который вы хотите перезагрузить.

5. В открывшемся окне подтверждения нажмите на кнопку **Перезагрузить**.

P2P-сервис будет перезагружен.

Удаление P2P-сервиса

Удаленные P2P-сервисы невозможно восстановить

Чтобы удалить P2P-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2P-сервисы**.

   Отобразится таблица P2P-сервисов.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с P2P-сервисом, который вы хотите удалить.

5. Если вы хотите удалить добавленные в P2P-сервис сервисные интерфейсы, в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**. Этот флажок снят по умолчанию.

6. Нажмите на кнопку **Удалить**.

P2P-сервис будет удален и перестанет отображаться в таблице.

Работа с транспортными сервисами Point-to-Multipoint (P2M)

Для просмотра таблицы P2M-сервисов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **P2M-сервисы**. Информация о P2M-сервисах отображается в следующих столбцах таблицы:

- **Имя** – имя P2M-сервиса.
- **Режим** – использование в P2M-сервисе DFI (Default Forwarding Inteface), на который отправляется неизвестный unicast-трафик:
  - **Классический** – не использовать DFI. Это значение выбрано по умолчанию.
  - **DFI с FIB на root и leafs** – использовать DFI на сервисном интерфейсе с ролью root.
  - **DFI с FIB на leaf** – использовать DFI на сервисном интерфейсе с ролью root. Сервисные интерфейсы с ролью leaf должны быть созданы на одном устройстве CPE. Резервные сервисные интерфейсы с ролью leaf должны быть созданы на одном устройстве CPE, отличном от устройства CPE, на котором созданы основные сервисные интерфейсы.
- **MAC-возраст (сек.)** – время в секундах, в течение которого записи хранятся в MAC-таблице контроллера.
- **Режим изучения MAC** – действие, которое применяется к серии кадров, когда первый кадр отправляется на контроллер для изучения MAC-адреса источника:
  - **Learn and flood** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отправляется на все добавленные в P2M-сервис сервисные интерфейсы, за исключением сервисного интерфейса, на который серия кадров пришла изначально.
  - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отбрасывается.

  При наличии MAC-адреса назначения в MAC-таблице серия кадров отправляется на сервисный интерфейс назначения.
- **Размер MAC-таблицы** – максимальное количество записей в MAC-таблице контроллера.

- **Перегрузка MAC-таблицы** – политика обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:
  - **Flood** – трафик с неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast).
  - **Drop** – трафик с неизученными MAC-адресами назначения не передается.
- **Выходные точки** – информация о сервисных интерфейсах, которые были добавлены в P2M-сервис:
  - Имена и идентификаторы DPID устройств CPE, на которых созданы сервисные интерфейсы.
  - Номера OpenFlow-портов, на которые ссылаются сервисные интерфейсы;
  - Роли сервисных интерфейсов:
    - **Root** – сервисный интерфейс может передавать трафик на сервисный интерфейс с любой ролью.
    - **Leaf** – сервисный интерфейс может передавать трафик только на сервисные интерфейсы с ролью **Root**.
- **Статус** – статус P2M-сервиса:
  - **Работает**.
  - **Не работает**.
- **Описание** – краткое описание P2M-сервиса.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание P2M-сервиса

Чтобы создать P2M-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

   Отобразится таблица P2M-сервисов.

4. В верхней части страницы нажмите на кнопку **+ P2M-сервис**.

5. В открывшемся окне в поле **Имя** введите имя P2M-сервиса.

6. В раскрывающемся списке **Ограничение** выберите созданное ограничение Manual-TE или пороговое ограничение, которое вы хотите добавить в P2M-сервис.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для распределения трафика по соединениям:

   - **По потокам** – потоки трафика (5-Tuple) распределяются по соединениям в соответствии со стоимостью соединений. Это значение выбрано по умолчанию.
   - **По пакетам** – пакеты трафика распределяются по соединениям в соответствии со стоимостью соединений.
   - **Широковещательный** – пакеты трафика дублируются и передаются одновременно через все соединения для исключения потерь.

   Вы можете указать стоимость соединения вручную.

8. При необходимости настройте режим адаптивной балансировки, если хотите, чтобы вес пути динамически корректировался в зависимости от уровня пакетных потерь на пути:

   a. Включите переключатель **Включить адаптивную балансировку**.

   b. В поле **Минимальный уровень потерь (%)** укажите минимальный процент пакетных потерь на пути, при котором режим адаптивной балансировки начинает влиять на вес. Диапазон значений: 0.01 – 100.

   c. В поле **Максимальный уровень потерь (%)** укажите максимальный процент пакетных потерь, при котором путь исключается из балансировки нагрузки.

   d. В раскрывающемся списке **Скорость схождения** выберите скорость схождения адаптивных весов к расчетным значениям:

      - **Fast** – 1;
      - **Fast** – 0,75;
      - **Fast** – 0,5.

9. В раскрывающемся списке **Режим** выберите, используется ли в P2M-сервисе DFI (Default Forwarding Interface), на который отправляется неизвестный unicast-трафик:

   - **Классический** – не использовать DFI. Это значение выбрано по умолчанию.
   - **DFI с FIB на root и leafs** – использовать DFI на сервисном интерфейсе с ролью root.
   - **DFI с FIB на leaf** – использовать DFI на сервисном интерфейсе с ролью root. Сервисные интерфейсы с ролью leaf должны быть созданы на одном устройстве CPE. Резервные сервисные интерфейсы с ролью leaf должны быть созданы на одном устройстве CPE, отличном от устройства CPE, на котором созданы основные сервисные интерфейсы.

10. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое применяется к серии кадров, когда первый кадр отправляется на контроллер для изучения MAC-адреса источника:

    - **Learn and flood** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отправляется на все добавленные в P2M-сервис сервисные интерфейсы, за исключением сервисного интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.

    - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отбрасывается.

    При наличии MAC-адреса назначения в MAC-таблице серия кадров отправляется на сервисный интерфейс назначения.

11. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. Значение по умолчанию: `300`.

12. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

    - **Flood** – трафик с неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.

    - **Drop** – трафик с неизученными MAC-адресами назначения не передается.

13. В поле **Размер MAC-таблицы** введите максимальное количество записей в MAC-таблице контроллера. Диапазон значений: от 0 до 65 535. Вы можете ввести `0`, чтобы не ограничивать количество записей в MAC-таблице контроллера. Значение по умолчанию: `100`.

14. При необходимости в поле **Описание** введите краткое описание P2M-сервиса.

15. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

16. Добавьте сервисный интерфейс в P2M-сервис:

    a. Нажмите на кнопку **+ Добавить**.

    Отобразятся параметры сервисного интерфейса.

    b. В раскрывающихся списках **Коммутатор** и **Сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите добавить в P2M-сервис.

    c. В раскрывающемся списке **QoS** выберите созданное правило качества обслуживания для сервисного интерфейса.

    d. В раскрывающемся списке **Входящий фильтр** выберите созданный фильтр трафика для сервисного интерфейса.

    e. В раскрывающемся списке **Роль** выберите роль сервисного интерфейса:

    - **Root** – сервисный интерфейс может передавать трафик на сервисный интерфейс с любой ролью.
    - **Leaf** – сервисный интерфейс может передавать трафик только на сервисные интерфейсы с ролью **Root**.
    - **Root, default forwarding interface** – сервисный интерфейс может передавать трафик на сервисный интерфейс с любой ролью и при этом сервисному интерфейсу назначена роль DFI.

    f. Если вы хотите добавить резервный сервисный интерфейс, через который трафик передается при выходе из строя основного сервисного интерфейса, в раскрывающихся списках **Резервный коммутатор** и **Резервный сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как резервный сервисный интерфейс.

    Если основной сервисный интерфейс возобновляет работу, P2M-сервис продолжает использовать резервный сервисный интерфейс.

    Сервисный интерфейс будет добавлен и отобразится в нижней части окна. Вы можете добавить несколько сервисных интерфейсов и удалить сервисные интерфейсы. Для удаления сервисного интерфейса нажмите рядом с ним на значок удаления ✕.

17. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

18. Если вы хотите добавить в P2M-сервис сразу несколько сервисных интерфейсов, вам нужно добавить группу OpenFlow-портов. Для этого выполните следующие действия:

    a. Нажмите на кнопку **+ Добавить**.

    Отобразятся параметры группы OpenFlow-портов.

    b. В раскрывающемся списке **Группа** выберите созданную группу OpenFlow-портов, которую вы хотите добавить в P2M-сервис. При сохранении параметров P2M-сервиса автоматически будут созданы сервисные интерфейсы, ссылающиеся на OpenFlow-порты в группе OpenFlow-портов, после чего сервисные интерфейсы будут автоматически добавлены в P2M-сервис.

    c. В раскрывающемся списке **QoS** выберите созданное правило качества обслуживания для автоматически созданных сервисных интерфейсов, ссылающихся на OpenFlow-порты.

    d. В поле **VLAN ID** введите значение внешней метки VLAN для автоматически созданных сервисных интерфейсов, ссылающихся на OpenFlow-порты. Поддерживается только автоматическое создание сервисных интерфейсов с типом классификации трафика VLAN. Каждому сервисному интерфейсу назначается одинаковая внешняя метка VLAN.

    e. В раскрывающемся списке **Роль** выберите роль для автоматически созданных сервисных интерфейсов, ссылающихся на OpenFlow-порты:

    - **Root** – сервисный интерфейс может передавать трафик на сервисный интерфейс с любой ролью.
    - **Leaf** – сервисный интерфейс может передавать трафик только на сервисные интерфейсы с ролью **Root**.

    Группа OpenFlow-портов будет добавлена и отобразится в нижней части окна. Вы можете добавить несколько групп OpenFlow-портов и удалить группы OpenFlow-портов. Для удаления группы OpenFlow-портов нажмите рядом с ней на значок удаления ✕.

19. Нажмите на кнопку **Создать**.

P2M-сервис будет создан и отобразится в таблице.

Просмотр статистики работы P2M-сервиса

Чтобы посмотреть статистику работы P2M-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

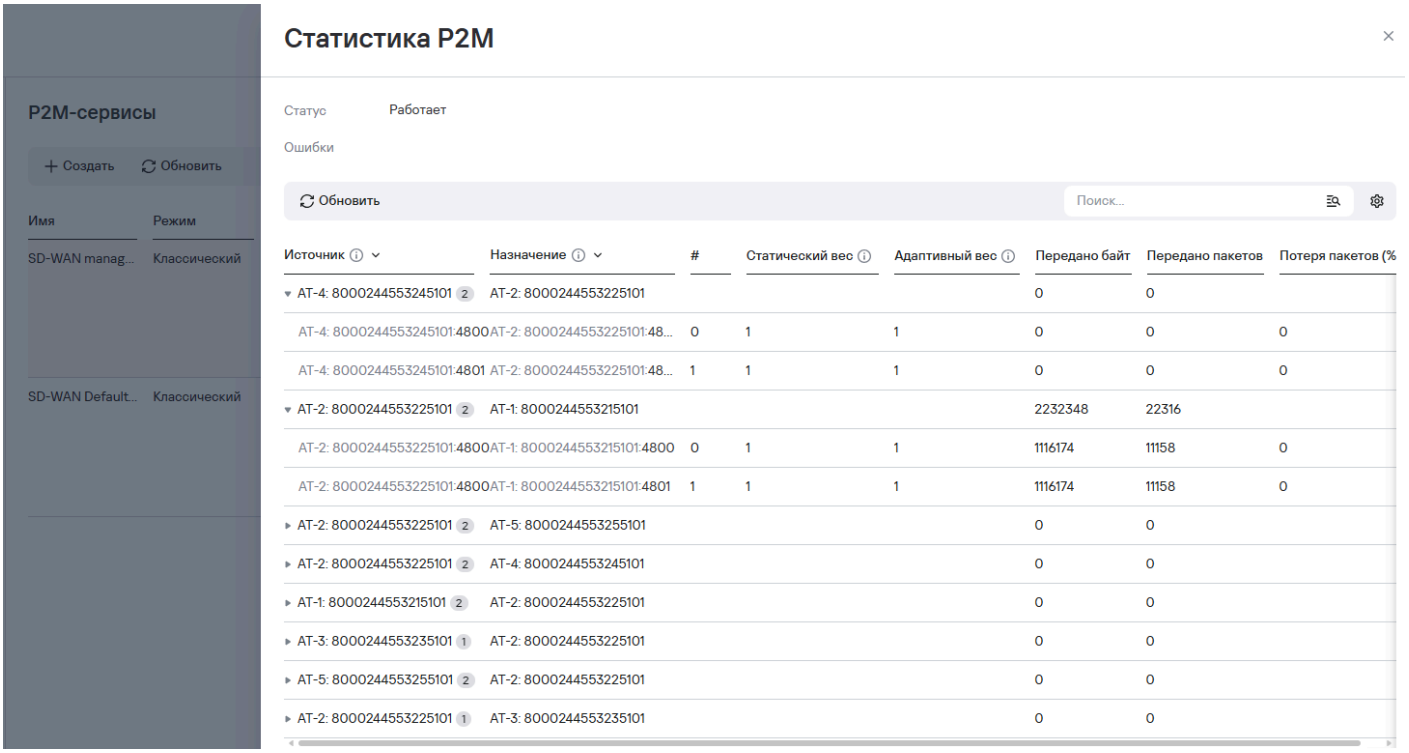
   Отобразится таблица P2M-сервисов.

4. Нажмите на кнопку **Управление** → **Статистика** рядом с P2M-сервисом, статистику работы которого вы хотите посмотреть.

Откроется окно со статистикой работы P2M-сервиса.

В верхней части окна статистики в поле **Статус** отображается операционный статус сервиса. В поле **Ошибки** показываются возможные ошибки, возникающие на сервисе.

Статистика по сегментам, путям и соединениям сервиса отображается в таблице в иерархическом виде. Строки в таблице сгруппированы по сегментам. Строки внутри каждой группы содержат статистику по путям, входящим в соответствующий сегмент. Группу можно раскрыть, нажав на треугольник (▸). У сервисов, для которых не заданы ограничения, в строках отображаются все пути с включенной в сегменте балансировкой нагрузки. У сервисов, для которых заданы ограничения, в строках отображаются пути Auto-TE, удовлетворяющие ограничению.



Отображение статистики на примере P2M-сервиса

Подробная информация статистики о сегментах и путях отображается в следующих столбцах таблицы:

Источник – для агрегирующих строк: исходный узел сегмента, для строк в раскрывающихся группах: исходный узел пути в сегменте.

Назначение – для агрегирующих строк: конечный узел сегмента, для строк в раскрывающихся группах: конечный узел пути в сегменте.

– порядковый номер пути. Чем меньше порядковый номер пути, тем раньше путь был построен. Значение отображается только у строк в раскрывающихся группах.

Статический вес – статический вес пути на основе стоимости. Значение отображается только у строк в раскрывающихся группах.

Адаптивный вес – динамический вес пути на основе анализа потерь пакетов на данном пути. Значение отображается только у строк в раскрывающихся группах. Если механизм адаптивной балансировки не используется, столбец не отображается.

Передано байт – для агрегирующих строк: значение из текущего окна статистики сервиса, для строк в раскрывающихся группах: количество переданных в бакет OF-группы байтов.

Передано пакетов – для агрегирующих строк: значение из текущего окна статистики сервиса, для строк в раскрывающихся группах: количество переданных в бакет OF-группы пакетов.

Потеря пакетов (%) – процентная потеря пакетов на данном пути (отношение количества потерянных пакетов к общему количеству отправленных пакетов). Значение отображается только у строк в раскрывающихся группах.

Просмотр MAC-таблицы P2M-сервиса

Чтобы посмотреть MAC-таблицу P2M-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

   Отобразится таблица P2M-сервисов.

4. Нажмите на кнопку **Управление** → **MAC-таблица** рядом с P2M-сервисом, MAC-таблицу которого вы хотите посмотреть.

   Откроется окно с MAC-таблицей P2M-сервиса. Информация о MAC-адресах отображается в следующих столбцах таблицы:

   - **MAC** – MAC-адрес.
   - **Имя хоста** – идентификатор DPID коммутатора, за которым находится MAC-адрес.
   - **Порт** – номер порта, за которым находится MAC-адрес.
   - **VLAN** – сегмент VLAN, в которой находится MAC-адрес.
   - **Возраст (сек.)** – время в секундах, на протяжении которого MAC-адрес находится в таблице MAC-адресов.

5. Если вы хотите найти MAC-адрес, введите его в поле и нажмите на кнопку **Найти по MAC**.

6. Если вы хотите очистить MAC-таблицу, нажмите на кнопку **Очистить**.

Просмотр и настройка отображения топологии P2M-сервиса

Чтобы посмотреть и настроить отображение топологии P2M-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

   Отобразится таблица P2M-сервисов.

4. Нажмите на кнопку **Управление** → **Топология сервиса** рядом с P2M-сервисом, топологию которого вы хотите посмотреть.

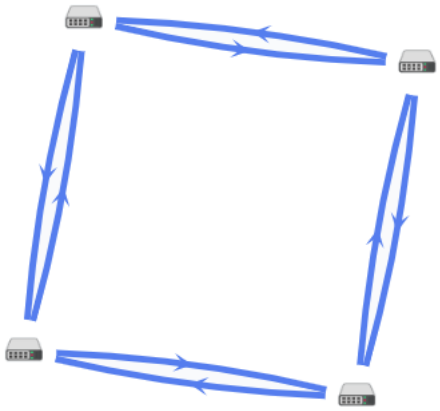
   Откроется окно с топологией P2M-сервиса.

5. При необходимости изменить расположение устройств CPE выполните одно из следующих действий:

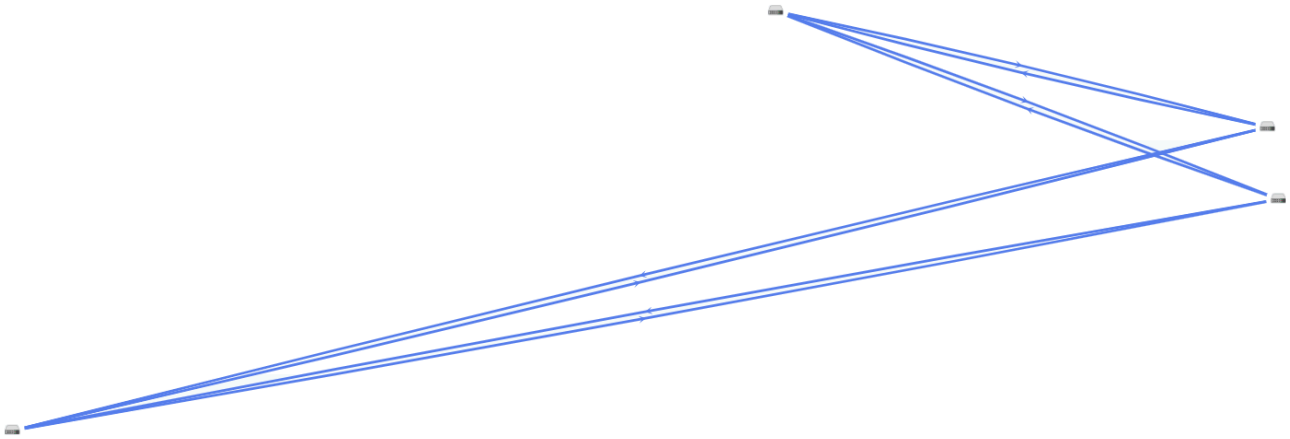
- Если вы хотите вручную изменить расположение устройств CPE, нажмите на кнопку **Вручную** и измените расположение устройств CPE.

- Если вы хотите автоматически расположить устройства CPE, нажмите на кнопку **Автоматически** и выберите одно из следующих значений в отобразившемся раскрывающемся списке:

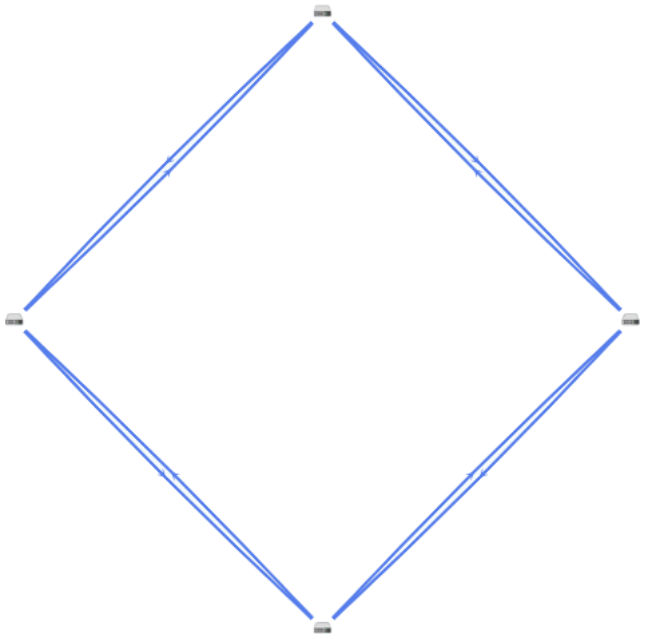
  - **Физическая симуляция** – устройства CPE располагаются примерно в соответствии с их реальным расположением относительно друг друга, например:



  - **Случайно** – устройства CPE располагаются случайным образом, например:

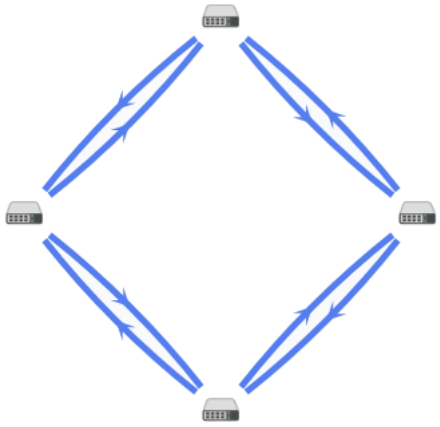


  - **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо, например:



- **Горизонтально** – устройства CPE располагаются горизонтально (в ширину), например:

- **Концентрически** – устройства CPE располагаются концентрически, например:



- **Решетка** – устройства CPE располагаются в соответствии с топологией решетка, например:

6. Если вы хотите отобразить информацию об устройствах CPE, установите следующие флажки:

   - **Имя** – отобразить имена устройств CPE.
   - **IP-адрес** – отобразить IP-адреса устройств CPE.

   По умолчанию флажки сняты.

7. Если вы хотите отобразить сегмент между двумя устройствами CPE, выполните следующие действия:

   a. Установите флажок **Сегменты**. Этот флажок снят по умолчанию.

   b. В отобразившихся раскрывающихся списках выберите устройство CPE источника и назначения сегмента.

   Отобразится сегмент между устройствами CPE.

Изменение P2M-сервиса

Чтобы изменить P2M-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

   Отобразится таблица P2M-сервисов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с P2M-сервисом, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры P2M-сервиса. Описание параметров см. в инструкции по созданию P2M-сервиса.

6. Нажмите на кнопку **Сохранить**.

P2M-сервис будет изменен и обновится в таблице.

Перезагрузка P2M-сервиса

Вы можете перезагрузить P2M-сервис, чтобы восстановить его работу при возникновении неполадок. Когда вы перезагружаете P2M-сервис, контроллер автоматически удаляет и повторно создает связанные с P2M-сервисом правила в OpenFlow-таблицах устройств CPE. Это затрагивает устройства CPE, сервисные интерфейсы которых добавлены в P2M-сервис.

Чтобы перезагрузить P2M-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

   Отобразится таблица P2M-сервисов.

4. Нажмите на кнопку **Управление** → **Перезагрузить** рядом с P2M-сервисом, который вы хотите перезагрузить.

5. В открывшемся окне подтверждения нажмите на кнопку **Подтвердить**.

P2M-сервис будет перезагружен.

Удаление P2M-сервиса

Удаленные P2M-сервисы невозможно восстановить.

Чтобы удалить P2M-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

   Отобразится таблица P2M-сервисов.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с P2M-сервисом, который вы хотите удалить.

5. Если вы хотите удалить добавленные в P2M-сервис сервисные интерфейсы, в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**. Этот флажок снят по умолчанию.

6. Нажмите на кнопку **Удалить**.

P2M-сервис будет удален и перестанет отображаться в таблице.

Работа с транспортными сервисами Multipoint-to-Multipoint (M2M)

Для просмотра таблицы M2M-сервисов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **M2M-сервисы**. Информация об M2M-сервисах отображается в следующих столбцах таблицы:

- **Имя** – имя M2M-сервиса.
- **MAC-возраст (сек.)** – время в секундах, в течение которого записи хранятся в MAC-таблице контроллера.
- **Режим изучения MAC** – действие, которое применяется к серии кадров, когда первый кадр отправляется на контроллер для изучения MAC-адреса источника:
  - **Learn and flood** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отправляется на все добавленные в M2M-сервис сервисные интерфейсы, за исключением сервисного интерфейса, на который серия кадров пришла изначально.
  - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отбрасывается.

  При наличии MAC-адреса назначения в MAC-таблице серия кадров отправляется на сервисный интерфейс назначения.
- **Размер MAC-таблицы** – максимальное количество записей в MAC-таблице контроллера.
- **Перегрузка MAC-таблицы** – политика обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:
  - **Flood** – трафик с неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.
  - **Drop** – трафик с неизученными MAC-адресами назначения не передается.

- **Выходные точки** – информация о сервисных интерфейсах, которые были добавлены в M2M-сервис:
  - имена и идентификаторы DPID устройств CPE, на которых созданы сервисные интерфейсы;
  - номера OpenFlow-портов, на которые ссылаются сервисные интерфейсы;
  - роли сервисных интерфейсов.
- **Статус** – статус M2M-сервиса:
  - **Работает**.
  - **Не работает**.
- **Описание** – краткое описание M2M-сервиса.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание M2M-сервиса

Чтобы создать M2M-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

   Отобразится таблица M2M-сервисов.

4. В верхней части страницы нажмите на кнопку **+ M2M-сервис**.

5. В открывшемся окне в поле **Имя** введите имя M2M-сервиса.

6. В раскрывающемся списке **Ограничение** выберите созданное ограничение Manual-TE или пороговое ограничение, которое вы хотите добавить в M2M-сервис.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для распределения трафика по соединениям:

   - **По потокам** – потоки трафика (5-Tuple) распределяются по соединениям в соответствии со стоимостью соединений. Это значение выбрано по умолчанию.
   - **По пакетам** – пакеты трафика распределяются по соединениям в соответствии со стоимостью соединений.
   - **Широковещательный** – пакеты трафика дублируются и передаются одновременно через все соединения для исключения потерь.

   Вы можете указать стоимость соединения вручную.

8. При необходимости настройте режим адаптивной балансировки, если хотите, чтобы вес пути динамически корректировался в зависимости от уровня пакетных потерь на пути:

   a. Включите переключатель **Включить адаптивную балансировку**.

   b. В поле **Минимальный уровень потерь (%)** укажите минимальный процент пакетных потерь на пути, при котором режим адаптивной балансировки начинает влиять на вес. Диапазон значений: 0.01 – 100.

   c. В поле **Максимальный уровень потерь (%)** укажите максимальный процент пакетных потерь, при котором путь исключается из балансировки нагрузки.

   d. В раскрывающемся списке **Скорость схождения** выберите скорость схождения адаптивных весов к расчетным значениям:

      - **Fast** – 1;
      - **Fast** – 0,75;
      - **Fast** – 0,5.

9. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое применяется к серии кадров, когда первый кадр отправляется на контроллер для изучения MAC-адреса источника:

   - **Learn and flood** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отправляется на все добавленные в M2M-сервис сервисные интерфейсы, за исключением сервисного интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.
   - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отбрасывается.

   При наличии MAC-адреса назначения в MAC-таблице серия кадров отправляется на сервисный интерфейс назначения.

10. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. Значение по умолчанию: `300`.

11. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

    - **Flood** – трафик с неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.
    - **Drop** – трафик с неизученными MAC-адресами назначения не передается.

12. В поле **Размер MAC-таблицы** введите максимальное количество записей в MAC-таблице контроллера. Диапазон значений: от 0 до 65 535. Вы можете ввести `0`, чтобы не ограничивать количество записей в MAC-таблице контроллера. Значение по умолчанию: `100`.

13. При необходимости в поле **Описание** введите краткое описание M2M-сервиса.

14. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

15. Добавьте сервисный интерфейс в M2M-сервис:

    a. Нажмите на кнопку **+ Добавить**.

    Отобразятся параметры сервисного интерфейса.

    b. В раскрывающихся списках **Коммутатор** и **Сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите добавить в M2M-сервис.

    c. В раскрывающемся списке **QoS** выберите созданное правило качества обслуживания для сервисного интерфейса.

    d. В раскрывающемся списке **Входящий фильтр** выберите созданный фильтр трафика для сервисного интерфейса.

    e. Если вы хотите добавить резервный сервисный интерфейс, через который трафик передается при выходе из строя основного сервисного интерфейса, в раскрывающихся списках **Резервный коммутатор** и **Резервный сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как резервный сервисный интерфейс.

    Если основной сервисный интерфейс возобновляет работу, M2M-сервис продолжает использовать резервный сервисный интерфейс.

    Сервисный интерфейс будет добавлен и отобразится в нижней части окна. Вы можете добавить несколько сервисных интерфейсов и удалить сервисные интерфейсы. Для удаления сервисного интерфейса нажмите рядом с ним на значок удаления ✕.

16. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

17. Если вы хотите добавить в M2M-сервис сразу несколько сервисных интерфейсов, вам нужно добавить группу OpenFlow-портов. Для этого выполните следующие действия:

    a. Нажмите на кнопку **+ Добавить**.

    Отобразятся параметры группы OpenFlow-портов.

    b. В раскрывающемся списке **Группа** выберите созданную группу OpenFlow-портов, которую вы хотите добавить в M2M-сервис. При сохранении параметров M2M-сервиса автоматически будут созданы сервисные интерфейсы, ссылающиеся на OpenFlow-порты в группе OpenFlow-портов, после чего эти сервисные интерфейсы будут автоматически добавлены в M2M-сервис.

    c. В раскрывающемся списке **QoS** выберите созданное правило качества обслуживания для автоматически созданных сервисных интерфейсов, ссылающихся на OpenFlow-порты.

    d. В поле **VLAN ID** введите значение внешней метки VLAN для автоматически созданных сервисных интерфейсов, ссылающихся на OpenFlow-порты. Поддерживается только автоматическое создание сервисных интерфейсов с типом классификации VLAN. Каждому сервисному интерфейсу назначается одинаковая внешняя метка VLAN.

    Группа OpenFlow-портов будет добавлена и отобразится в нижней части окна. Вы можете добавить несколько групп OpenFlow-портов и удалить группы OpenFlow-портов. Для удаления группы OpenFlow-портов нажмите рядом с ней на значок удаления ✕.

18. Нажмите на кнопку **Создать**.

M2M-сервис будет создан и отобразится в таблице.

Просмотр статистики работы M2M-сервиса

Чтобы посмотреть статистику работы M2M-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

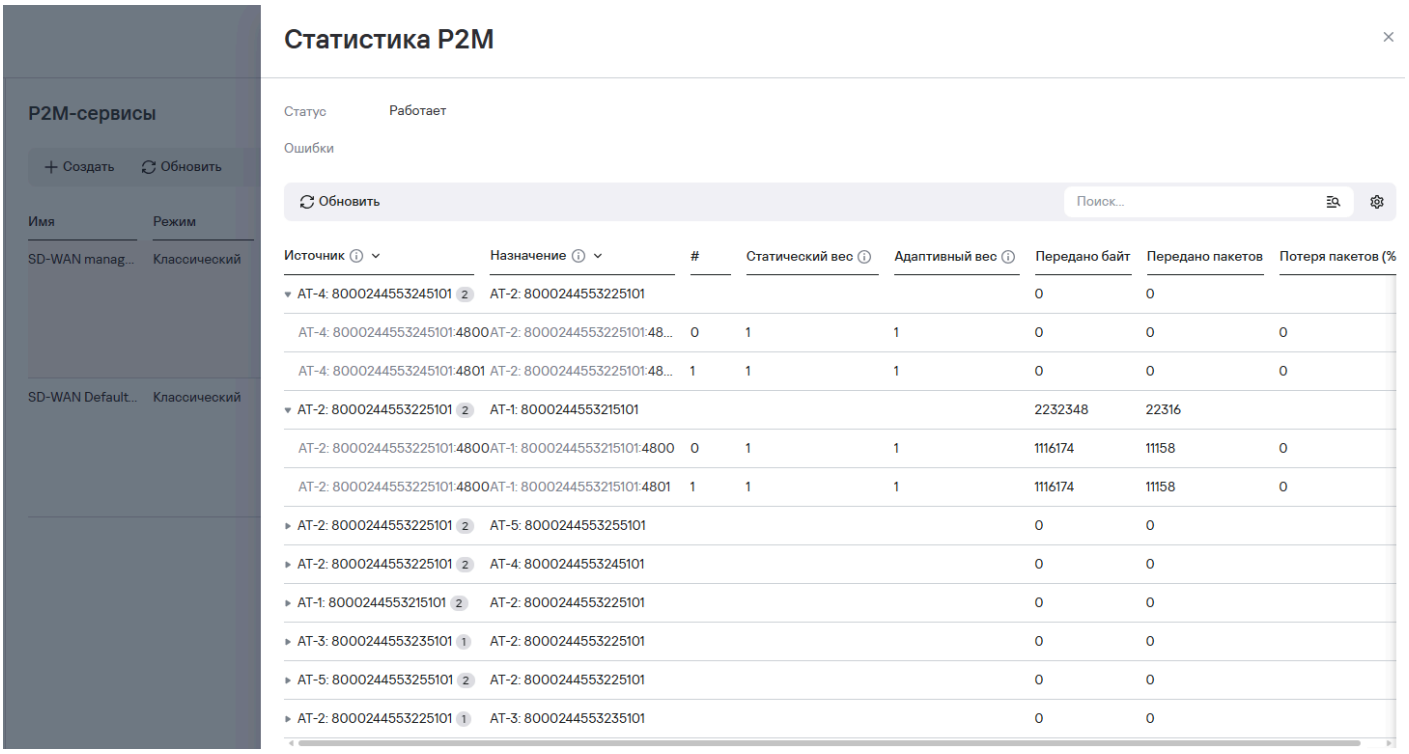
   Отобразится таблица M2M-сервисов.

4. Нажмите на кнопку **Управление** → **Статистика** рядом с M2M-сервисом, статистику работы которого вы хотите посмотреть.

Откроется окно со статистикой работы M2M-сервиса.

В верхней части окна статистики в поле **Статус** отображается операционный статус сервиса. В поле **Ошибки** показываются возможные ошибки, возникающие на сервисе.

Статистика по сегментам, путям и соединениям сервиса отображается в таблице в иерархическом виде. Строки в таблице сгруппированы по сегментам. Строки внутри каждой группы содержат статистику по путям, входящим в соответствующий сегмент. Группу можно раскрыть, нажав на треугольник (▸). У сервисов, для которых не заданы ограничения, в строках отображаются все пути с включенной в сегменте балансировкой нагрузки. У сервисов, для которых заданы ограничения, в строках отображаются пути Auto-TE, удовлетворяющие ограничению.



Отображение статистики на примере P2M-сервиса

Подробная информация статистики о сегментах и путях отображается в следующих столбцах таблицы:

Источник – для агрегирующих строк: исходный узел сегмента, для строк в раскрывающихся группах: исходный узел пути в сегменте.

Назначение – для агрегирующих строк: конечный узел сегмента, для строк в раскрывающихся группах: конечный узел пути в сегменте.

– порядковый номер пути. Чем меньше порядковый номер пути, тем раньше путь был построен. Значение отображается только у строк в раскрывающихся группах.

Статический вес – статический вес пути на основе стоимости. Значение отображается только у строк в раскрывающихся группах.

Адаптивный вес – динамический вес пути на основе анализа потерь пакетов на данном пути. Значение отображается только у строк в раскрывающихся группах. Если механизм адаптивной балансировки не используется, столбец не отображается.

Передано байт – для агрегирующих строк: значение из текущего окна статистики сервиса, для строк в раскрывающихся группах: количество переданных в бакет OF-группы байтов.

Передано пакетов – для агрегирующих строк: значение из текущего окна статистики сервиса, для строк в раскрывающихся группах: количество переданных в бакет OF-группы пакетов.

Потеря пакетов (%) – процентная потеря пакетов на данном пути (отношение количества потерянных пакетов к общему количеству отправленных пакетов). Значение отображается только у строк в раскрывающихся группах.

Просмотр MAC-таблицы M2M-сервиса

Чтобы посмотреть MAC-таблицу M2M-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

   Отобразится таблица M2M-сервисов.

4. Нажмите на кнопку **Управление** → **MAC-таблица** рядом с M2M-сервисом, MAC-таблицу которого вы хотите посмотреть.

   Откроется окно с MAC-таблицей M2M-сервиса. Информация о MAC-адресах отображается в следующих столбцах таблицы:

   - **MAC** – MAC-адрес.
   - **Имя хоста** – идентификатор DPID коммутатора, за которым находится MAC-адрес.
   - **Порт** – номер порта, за которым находится MAC-адрес.
   - **VLAN** – сегмент VLAN, в которой находится MAC-адрес.
   - **Возраст (сек.)** – время в секундах, на протяжении которого MAC-адрес находится в таблице MAC-адресов.

5. Если вы хотите найти MAC-адрес, введите его в поле и нажмите на кнопку **Найти по MAC**.

6. Если вы хотите очистить MAC-таблицу, нажмите на кнопку **Очистить**.

Просмотр и настройка отображения топологии M2M-сервиса

Чтобы посмотреть и настроить отображение топологии M2M-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

   Отобразится таблица M2M-сервисов.

4. Нажмите на кнопку **Управление** → **Топология сервиса** рядом с M2M-сервисом, топологию которого вы хотите посмотреть.

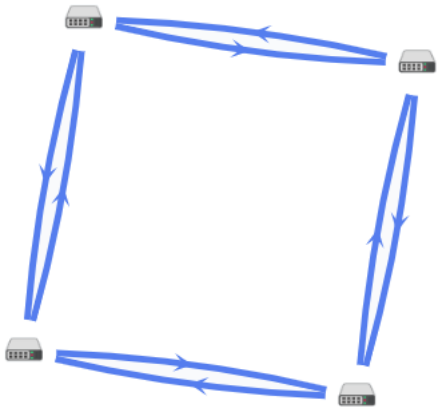
   Откроется окно с топологией M2M-сервиса.

5. При необходимости изменить расположение устройств CPE выполните одно из следующих действий:

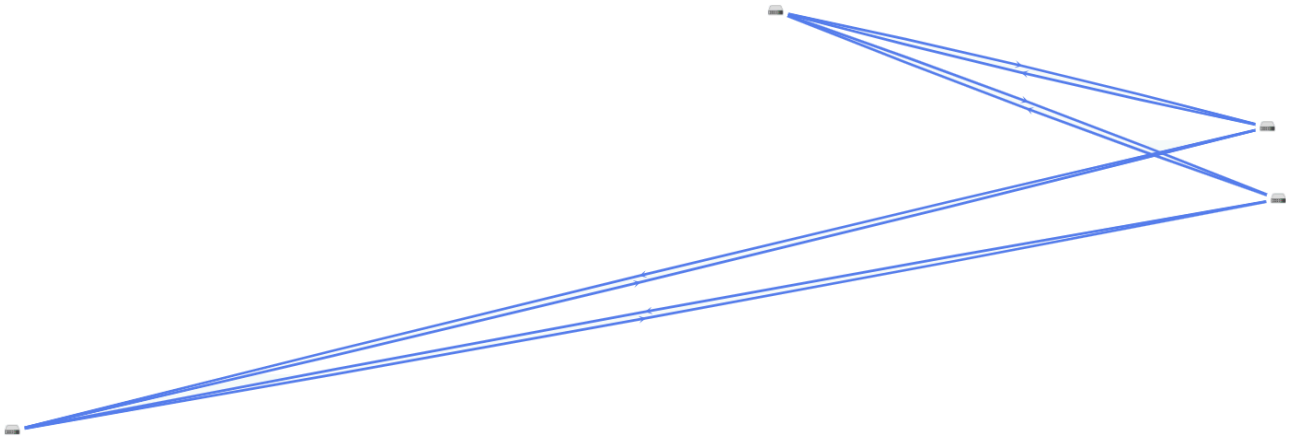
- Если вы хотите вручную изменить расположение устройств CPE, нажмите на кнопку **Вручную** и измените расположение устройств CPE.

- Если вы хотите автоматически расположить устройства CPE, нажмите на кнопку **Автоматически** и выберите одно из следующих значений в отобразившемся раскрывающемся списке:

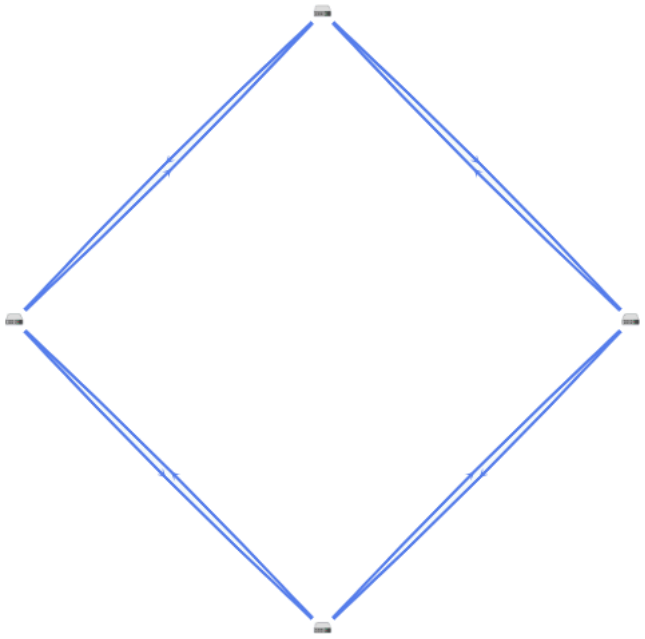
  - **Физическая симуляция** – устройства CPE располагаются примерно в соответствии с их реальным расположением относительно друг друга, например:



  - **Случайно** – устройства CPE располагаются случайным образом, например:

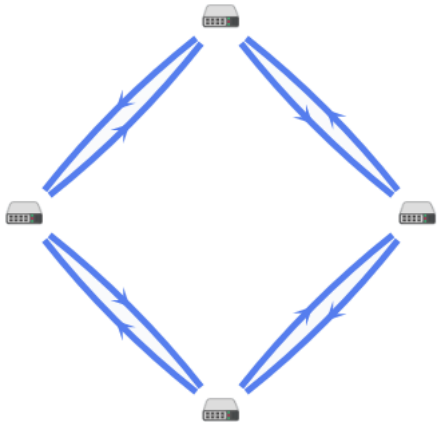


  - **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо, например:



- **Горизонтально** – устройства CPE располагаются горизонтально (в ширину), например:

- **Концентрически** – устройства CPE располагаются концентрически, например:



- **Решетка** – устройства CPE располагаются в соответствии с топологией решетка, например:

6. Если вы хотите отобразить информацию об устройствах CPE, установите следующие флажки:

   - **Имя** – отобразить имена устройств CPE.
   - **IP-адрес** – отобразить IP-адреса устройств CPE.

   По умолчанию флажки сняты.

7. Если вы хотите отобразить сегмент между двумя устройствами CPE, выполните следующие действия:

   a. Установите флажок **Сегменты**. Этот флажок снят по умолчанию.

   b. В отобразившихся раскрывающихся списках выберите устройство CPE источника и назначения сегмента.

   Отобразится сегмент между устройствами CPE.

Изменение M2M-сервиса

Чтобы изменить M2M-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

   Отобразится таблица M2M-сервисов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с M2M-сервисом, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры M2M-сервиса. Описание параметров см. в инструкции по созданию M2M-сервиса.

6. Нажмите на кнопку **Сохранить**.

M2M-сервис будет изменен и обновится в таблице.

Перезагрузка M2M-сервиса

Вы можете перезагрузить M2M-сервис, чтобы восстановить его работу при возникновении неполадок. Когда вы перезагружаете M2M-сервис, контроллер автоматически удаляет и повторно создает связанные с M2M-сервисом правила в OpenFlow-таблицах устройств CPE. Это затрагивает устройства CPE, сервисные интерфейсы которых добавлены в M2M-сервис.

Чтобы перезагрузить M2M-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

   Отобразится таблица M2M-сервисов.

4. Нажмите на кнопку **Управление** → **Перезагрузить** рядом с M2M-сервисом, который вы хотите перезагрузить.

5. В открывшемся окне подтверждения нажмите на кнопку **Подтвердить**.

M2M-сервис будет перезагружен.

Удаление M2M-сервиса

Удаленные M2M-сервисы невозможно восстановить.

Чтобы удалить M2M-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

   Отобразится таблица M2M-сервисов.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с M2M-сервисом, который вы хотите удалить.

5. Если вы хотите удалить добавленные в M2M-сервис сервисные интерфейсы, в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**. Этот флажок снят по умолчанию.

6. Нажмите на кнопку **Удалить**.

M2M-сервис будет удален перестанет отображаться в таблице.

Работа с транспортными сервисами IP multicast

Для просмотра таблицы IP multicast-сервисов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **IP multicast-сервисы**. Информация об IP multicast-сервисах отображается в следующих столбцах таблицы:

- **Имя** – имя IP multicast-сервиса.
- **Сервисный интерфейс источника** – информация о сервисном интерфейсе источника IP multicast-сервиса:
  - имя и идентификатор DPID устройства CPE, на котором создан сервисный интерфейс;
  - номер OpenFlow-порта, на который ссылается сервисный интерфейс.
- **Резервный сервисный интерфейс** – информация о резервном сервисном интерфейсе источника IP multicast-сервиса:
  - имя и идентификатор DPID устройства CPE, на котором создан сервисный интерфейс;
  - номер OpenFlow-порта, на который ссылается сервисный интерфейс.
- **IP запросчика** – IP-адрес сервисного интерфейса источника IP multicast-сервиса.
- **Сервисные интерфейсы-подписчики** – информация о сервисных интерфейсах назначения IP multicast-сервиса:
  - имена и идентификаторы DPID устройств CPE, на которых созданы сервисные интерфейсы;
  - номера OpenFlow-портов, на которые ссылаются сервисные интерфейсы.
- **Группы** – информация о multicast-группах, которые были добавлены в IP multicast-сервис:
  - IP-адреса multicast-групп;
  - длины префиксов multicast-групп;
  - гарантированная скорость передачи для multicast-групп.

- **Статус** – статус IP multicast-сервиса:
  - **Работает**.
  - **Не работает**.
- **Ошибки** – ошибки, возникшие при работе IP multicast-сервиса.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание IP multicast-сервиса

Чтобы создать IP multicast-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **IP multicast-сервисы**.

   Отобразится таблица IP multicast-сервисов.

4. В верхней части страницы нажмите на кнопку **+ IP multicast-сервис**.

5. В открывшемся окне в поле **Имя** введите имя IP multicast-сервиса.

6. В раскрывающихся списках **Коммутатор источника** и **Сервисный интерфейс источника** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как сервисный интерфейс источника IP multicast-сервиса.

7. Если вы хотите отобразить в раскрывающемся списке **Сервисный интерфейс источника** сервисные интерфейсы, которые добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. Этот флажок снят по умолчанию.

8. В поле **IP запросчика** введите IP-адрес сервисного интерфейса источника IP multicast-сервиса.

9. Если вы хотите добавить резервный сервисный интерфейс источника IP multicast-сервиса, через который трафик передается при выходе из строя основного сервисного интерфейса, выполните следующие действия:

    a. Установите флажок **Резервный интерфейс**. Этот флажок снят по умолчанию.

    b. В раскрывающихся списках **Резервный коммутатор** и **Резервный сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как резервный сервисный интерфейс.

    c. Если вы хотите отобразить в раскрывающемся списке **Резервный сервисный интерфейс** сервисные интерфейсы, которые добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. Этот флажок снят по умолчанию.

    d. Если вы хотите, чтобы IP multicast-сервис снова использовал основной сервисный интерфейс источника при возобновлении работы сервисного интерфейса, установите флажок **Автовозвращение при восстановлении**. Этот флажок снят по умолчанию.

    e. Если вы хотите, чтобы на резервном сервисном интерфейсе строилось дерево распространения multicast-трафика, установите флажок **Резервное multicast-дерево**. Пакеты трафика отбрасываются на резервном сервисном интерфейсе, пока основной остается активным. Этот флажок установлен по умолчанию.

10. Установите флажок **IGMP-прокси**, чтобы использовать прокси-сервер IGMP. Это позволяет сохранить передачу трафика на активные multicast-группы, к которым подключен хотя бы один сервисный интерфейс назначения IP multicast-сервиса. Этот флажок снят по умолчанию.

11. В раскрывающемся списке **QoS** выберите созданное правило качества обслуживания для сервисного интерфейса источника IP multicast-сервиса.

12. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

13. Добавьте сервисный интерфейс назначения в IP multicast-сервис:

    a. В раскрывающихся списках **Коммутатор подписчика** и **Сервисный интерфейс подписчика** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как сервисный интерфейс назначения IP multicast-сервиса.

    b. Если вы хотите отобразить в раскрывающемся списке **Сервисный интерфейс подписчика** сервисные интерфейсы, которые добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. Этот флажок снят по умолчанию.

    c. Нажмите на кнопку **+ Добавить**.

    Сервисный интерфейс будет добавлен и отобразится в нижней части окна. Вы можете добавить несколько сервисных интерфейсов и удалить сервисные интерфейсы. Для удаления сервисного интерфейса нажмите рядом с ним на кнопку **Удалить**.

14. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

15. Добавьте multicast-группу в IP multicast-сервис:

    a. В поле **IP-адрес** введите IP-адрес multicast-группы. Диапазон значений: от 224.0.0.0 до 239.255.255.255.

    b. В раскрывающемся списке **Маска** выберите длину префикса multicast-группы. Диапазон значений: от 24 до 32.

    c. В раскрывающемся списке **GBR** выберите гарантированную скорость передачи (англ. Guaranteed Bit Rate, GBR) для multicast-группы.

    d. Нажмите на кнопку **+ Добавить**.

    Multicast-группа будет добавлена и отобразится в нижней части окна. Вы можете добавить несколько multicast-групп и удалить multicast-группы. Для удаления multicast-группы нажмите рядом с ней на кнопку **Удалить**.

16. Нажмите на кнопку **Создать**.

IP multicast-сервис будет создан и отобразится в таблице.

Просмотр статистики работы IP multicast-сервиса

Чтобы посмотреть статистику работы IP multicast-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **IP multicast-сервисы**.

   Отобразится таблица IP multicast-сервисов.

4. Нажмите на кнопку **Управление** → **Статистика** рядом с IP multicast-сервисом, статистику работы которого вы хотите посмотреть.

Откроется окно со статистикой работы IP multicast-сервиса.

Изменение IP multicast-сервиса

Чтобы изменить IP multicast-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **IP multicast-сервисы**.

   Отобразится таблица IP multicast-сервисов.

4. Нажмите на кнопку **Управление** → **Изменить интерфейсы источника**, **Изменить интерфейсы подписчика** или **Изменить multicast-группы** рядом с IP multicast-сервисом, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры IP multicast-сервиса. Описание параметров см. в инструкции по созданию IP multicast-сервиса.

6. Нажмите на кнопку **Сохранить**.

IP multicast-сервис будет изменен и обновится в таблице.

Удаление IP multicast-сервиса

Удаленные IP multicast-сервисы невозможно восстановить.

Чтобы удалить IP multicast-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **IP multicast-сервисы**.

   Отобразится таблица IP multicast-сервисов.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с IP multicast-сервисом, который вы хотите удалить.

5. Если вы хотите удалить добавленные в IP multicast-сервис сервисные интерфейсы, в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**. Этот флажок снят по умолчанию.

6. Нажмите на кнопку **Удалить**.

IP multicast-сервис будет удален и перестанет отображаться в таблице.

Работа с транспортными сервисами L3 VPN

Для просмотра таблицы L3 VPN-сервисов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **L3 VPN-сервисы**. Информация об L3 VPN-сервисах отображается в следующих столбцах таблицы:

- **Имя** – имя L3 VPN-сервиса.
- **Тип** – тип топологии L3 VPN-сервиса.
- **Inter-spoke через hub** – между площадками может устанавливаться связь через центральную площадку:
  - **Да**.
  - **Нет**.
- **Выходные точки** – информация об L3-интерфейсах, которые были добавлены в L3 VPN-сервис:
  - Если L3-интерфейсы ссылаются на M2M-сервисы, отображаются имена M2M-сервисов;
  - Если L3-интерфейсы ссылаются на сервисные интерфейсы, отображается следующая информация:
    - имена и идентификаторы DPID устройств CPE, на которых созданы сервисные интерфейсы;
    - номера OpenFlow-портов, на которые ссылаются сервисные интерфейсы;
    - правила качества обслуживания, указанные для сервисных интерфейсов;
    - фильтры трафика, указанные для сервисных интерфейсов.
  - Длины префиксов L3-интерфейсов.
  - MAC-адреса L3-интерфейсов.
  - Время в секундах, в течение которого записи хранятся в ARP-таблице на контроллере.

- **Маршруты** – информация о статических маршрутах, которые были добавлены в L3 VPN-сервис:
  - IPv4-префиксы назначения статических маршрутов;
  - IPv4-адреса шлюзов для маршрутизации пакетов трафика на IPv4-префиксы назначения статических маршрутов;
  - L3-интерфейсы, за которыми находятся IPv4-префиксы назначения статических маршрутов;
  - метрики статических маршрутов.
- **Статус** – статус L3 VPN-сервиса:
  - **Работает**.
  - **Не работает**.
- **Ошибки** – ошибки, возникшие при работе L3 VPN-сервиса.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание L3 VPN-сервиса

Чтобы создать L3 VPN-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. В верхней части страницы нажмите на кнопку **+ L3 VPN-сервис**.

5. В открывшемся окне в поле **Имя** введите имя L3 VPN-сервиса.

6. В раскрывающемся списке **Ограничение** выберите созданное ограничение Manual-TE или пороговое ограничение, которое вы хотите добавить в L3 VPN-сервис.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для распределения трафика по соединениям:

   - **По потокам** – потоки трафика (5-Tuple) распределяются по соединениям в соответствии со стоимостью соединений. Это значение выбрано по умолчанию.
   - **По пакетам** – пакеты трафика распределяются по соединениям в соответствии со стоимостью соединений.
   - **Широковещательный** – пакеты трафика дублируются и передаются одновременно через все соединения для исключения потерь.

   Вы можете указать стоимость соединения вручную.

8. При необходимости настройте режим адаптивной балансировки, если хотите, чтобы вес пути динамически корректировался в зависимости от уровня пакетных потерь на пути:

   a. Включите переключатель **Включить адаптивную балансировку**.

   b. В поле **Минимальный уровень потерь (%)** укажите минимальный процент пакетных потерь на пути, при котором режим адаптивной балансировки начинает влиять на вес. Диапазон значений: 0.01 – 100.

   c. В поле **Максимальный уровень потерь (%)** укажите максимальный процент пакетных потерь, при котором путь исключается из балансировки нагрузки.

   d. В раскрывающемся списке **Скорость схождения** выберите скорость схождения адаптивных весов к расчетным значениям:

      - **Fast** – 1;
      - **Fast** – 0,75;
      - **Fast** – 0,5.

9. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

10. Добавьте L3-интерфейс в L3 VPN-сервис:

    a. В раскрывающемся списке **Режим** выберите тип L3-интерфейса:

    - **M2M-сервис** – L3-интерфейс ссылается на M2M-сервис.
    - **Сервисный интерфейс** – L3-интерфейс ссылается на сервисный интерфейс.

    b. Если в раскрывающемся списке **Режим** вы выбрали **M2M-сервис**, в раскрывающемся списке **M2M-сервис** выберите созданный M2M-сервис, на который ссылается L3-интерфейс.

    c. Если в раскрывающемся списке **Режим** вы выбрали **Сервисный интерфейс**, настройте сервисный интерфейс:

    1. В раскрывающихся списках **Коммутатор** и **Сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, на который ссылается L3-интерфейс.
    2. В раскрывающемся списке **QoS** выберите созданное правило качества обслуживания для L3-интерфейса.
    3. В раскрывающемся списке **Входящий фильтр** выберите созданный фильтр трафика для L3-интерфейса.
    4. Если вы хотите отобразить в раскрывающемся списке **Сервисный интерфейс** сервисные интерфейсы, которые добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. Этот флажок снят по умолчанию.

    d. В поле **IP** введите IP-адрес L3-интерфейса.

    e. В поле **Длина префикса** введите длину префикса L3-интерфейса. Диапазон значений: от 0 до 32.

    f. В поле **MAC-адрес** введите MAC-адрес L3-интерфейса. Вы можете сгенерировать MAC-адрес, нажав на кнопку **Сгенерировать**.

    g. В поле **APR-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в ARP-таблице L3 VPN-сервиса. Диапазон значений: от 1 до 65 535. Значение по умолчанию: `200`.

    h. Нажмите на кнопку **+ Добавить**.

    L3-интерфейс будет добавлен и отобразится в нижней части окна. Вы можете добавить несколько L3-интерфейсов и удалить L3-интерфейсы. Для удаления L3-интерфейса нажмите рядом с ним на кнопку **Удалить**.

11. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

12. Если вы хотите добавить статический маршрут в L3 VPN-сервис, выполните следующие действия:

    a. В поле **IP** введите IPv4-адрес назначения статического маршрута.

    b. В поле **Длина префикса** введите длину IPv4-префикса назначения статического маршрута. Диапазон значений: от 0 до 32.

    c. В раскрывающемся списке **SVI** выберите добавленный L3-интерфейс, за которым находится IPv4-префикс назначения статического маршрута. Вы добавили L3-интерфейс на шаге 9 этой инструкции.

    d. В поле **Шлюз** введите IPv4-адрес шлюза для маршрутизации пакетов трафика на IPv4-префикс назначения статического маршрута.

    e. В поле **Метрика** введите метрику статического маршрута. Значение по умолчанию: `0`.

    f. Нажмите на кнопку **+ Добавить**.

    Статический маршрут будет добавлен и отобразится в нижней части окна. Вы можете добавить несколько статических маршрутов и удалить статические маршруты. Для удаления статического маршрута нажмите рядом с ним на кнопку **Удалить**.

13. Нажмите на кнопку **Создать**.

    L3 VPN-сервис будет создан и отобразится в таблице.

Работа с ARP-таблицей L3 VPN-сервиса

Для просмотра ARP-таблицы L3 VPN-сервиса вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейти в раздел **L3 VPN-сервисы** и нажать на кнопку **Управление** → **ARP-таблица** рядом с L3 VPN-сервисом. Информация записях отображается в следующих столбцах таблицы:

- **IP** – IP-адрес сервисного интерфейса.
- **MAC** – MAC-адрес сервисного интерфейса.
- **Сервисный интерфейс** – информация о сервисном интерфейсе:
  - имя и идентификатор DPID устройства CPE, на котором создан сервисный интерфейс;
  - номер OpenFlow-порта, на который ссылается сервисный интерфейс.
- **Время жизни (сек.)** – время в секундах, которое прошло с момента создания записи.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание статической записи в ARP-таблице L3 VPN-сервиса

Чтобы создать статическую запись в ARP-таблице L3 VPN-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. Нажмите на кнопку **Управление** → **ARP-таблица** рядом с L3 VPN-сервисом, в ARP-таблице которого вы хотите создать статическую запись.

   Откроется страница с ARP-таблицей L3 VPN-сервиса.

5. В верхней части страницы нажмите на кнопку **+ Статическая ARP-запись**.

6. В открывшемся окне в раскрывающихся списках **Коммутатор** и **Сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, для которого вы хотите указать IP-адрес и MAC-адрес.

7. В поле **IP-адрес** введите IP-адрес сервисного интерфейса.

8. В поле **MAC** введите MAC-адрес сервисного интерфейса.

9. Нажмите на кнопку **Создать**.

Статическая запись будет создана и отобразится в ARP-таблице L3 VPN-сервиса.

Изменение статической записи в ARP-таблице L3 VPN-сервиса

Чтобы изменить статическую запись в ARP-таблице L3 VPN-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. Нажмите на кнопку **Управление** → **ARP-таблица** рядом с L3 VPN-сервисом, в ARP-таблице которого вы хотите изменить статическую запись.

   Откроется страница с ARP-таблицей L3 VPN-сервиса.

5. Нажмите на кнопку **Управление** → **Изменить** рядом со статической записью, которую вы хотите изменить.

6. В открывшемся окне при необходимости измените IP-адрес и/или MAC-адрес сервисного интерфейса.

7. Нажмите на кнопку **Сохранить**.

Статическая запись будет изменена и обновится в таблице.

Удаление статической записи в ARP-таблице L3 VPN-сервиса

Удаленные статические записи в ARP-таблице L3 VPN-сервиса невозможно восстановить.

Чтобы удалить статическую запись в ARP-таблице L3 VPN-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. Нажмите на кнопку **Управление** → **ARP-таблица** рядом с L3 VPN-сервисом, в ARP-таблице которого вы хотите удалить статическую запись.

   Откроется страница с ARP-таблицей L3 VPN-сервиса.

5. Нажмите на кнопку **Управление** → **Удалить** рядом со статической записью, которую вы хотите удалить.

6. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Статическая запись будет удалена и перестанет отображаться в таблице.

Просмотр таблицы маршрутизации L3 VPN-сервиса

Чтобы посмотреть таблицу маршрутизации L3 VPN-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. Нажмите на кнопку **Управление** → **Таблица маршрутизации** рядом с L3 VPN-сервисом, таблицу маршрутизации которого вы хотите посмотреть.

Откроется окно с таблицей маршрутизации L3 VPN-сервиса.

Изменение L3 VPN-сервиса

Чтобы изменить L3 VPN-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с L3 VPN-сервисом, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры L3 VPN-сервиса. Описание параметров см. в инструкции по созданию L3 VPN-сервиса.

6. Нажмите на кнопку **Сохранить**.

L3 VPN-сервис будет изменен и обновится в таблице.

Перезагрузка L3 VPN-сервиса

Вы можете перезагрузить L3 VPN-сервис, чтобы восстановить его работу при возникновении неполадок. Когда вы перезагружаете L3 VPN-сервис, контроллер автоматически удаляет и повторно создает связанные с L3 VPN-сервисом правила в OpenFlow-таблицах устройств CPE. Это затрагивает устройства CPE, сервисные интерфейсы которых добавлены в L3 VPN-сервис.

Чтобы перезагрузить L3 VPN-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. Нажмите на кнопку **Управление** → **Перезагрузить** рядом с L3 VPN-сервисом, который вы хотите перезагрузить.

5. В открывшемся окне подтверждения нажмите на кнопку **Подтвердить**.

L3 VPN-сервис будет перезагружен.

Удаление L3 VPN-сервиса

Удаленные L3 VPN-сервисы невозможно восстановить.

Чтобы удалить L3 VPN-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. Нажмите на кнопку **Управление** → **Удалить** рядом с L3 VPN-сервисом, который вы хотите удалить.

5. Если вы хотите удалить добавленные в L3 VPN-сервис сервисные интерфейсы, в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**. Этот флажок снят по умолчанию.

6. Нажмите на кнопку **Удалить**.

L3 VPN-сервис будет удален и перестанет отображаться в таблице.

Работа с транспортными сервисами в шаблоне экземпляра SD-WAN

Для просмотра таблицы P2M-сервисов и M2M-сервисов в шаблоне экземпляра SD-WAN вам нужно в меню перейти в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**, нажать на шаблон экземпляра SD-WAN и выбрать вкладку **Транспортные сервисы**. Информация о P2M-сервисах и M2M-сервисах отображается в следующих столбцах таблицы:

- **Имя** – имя P2M-сервиса или M2M-сервиса.
- **Тип** – тип транспортного сервиса:
  - **P2M**.
  - **M2M**.
- **Управляющий транспортный сервис** – P2M-сервис или M2M-сервис является управляющим:
  - **Да**.
  - **Нет**.
- **Режим** – использование в P2M-сервисе DFI (Default Forwarding Inteface), на который отправляется неизвестный unicast-трафик:
  - **Классический** – не использовать DFI. Это значение выбрано по умолчанию.
  - **DFI с FIB на root и leafs** – использовать DFI на сервисном интерфейсе с ролью root.
  - **DFI с FIB на leaf** – использовать DFI на сервисном интерфейсе с ролью root. Сервисные интерфейсы с ролью leaf должны быть созданы на одном устройстве CPE. Резервные сервисные интерфейсы с ролью leaf должны быть созданы на одном устройстве CPE, отличном от устройства CPE, на котором созданы основные сервисные интерфейсы.

  Значение в этом столбце отображается, только если в столбце **Тип** отображается значение **P2M**.
- **MAC-возраст (сек.)** – время в секундах, в течение которого записи хранятся в MAC-таблице контроллера.

- **Режим изучения MAC** – действие, которое применяется к серии кадров, когда первый кадр отправляется на контроллер для изучения MAC-адреса источника:

  - **Learn and flood** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отправляется на все добавленные в M2M-сервис сервисные интерфейсы, за исключением сервисного интерфейса, на который серия кадров пришла изначально.

  - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отбрасывается.

  При наличии MAC-адреса назначения в MAC-таблице серия кадров отправляется на сервисный интерфейс назначения.

- **Размер MAC-таблицы** – максимальное количество записей в MAC-таблице контроллера.

- **Перегрузка MAC-таблицы** – политика обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

  - **Flood** – трафик с неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.

  - **Drop** – трафик с неизученными MAC-адресами назначения не передается.

- **Действия** – действия, которые можно выполнить с транспортным сервисом.

Для просмотра списка L3 VPN-сервисов вам нужно выбрать вкладку **L3-сервисы**.

Создание P2M-сервиса или M2M-сервиса в шаблоне экземпляра SD-WAN

Чтобы создать P2M-сервис или M2M-сервис в шаблоне экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, в котором вы хотите создать P2M-сервис или M2M-сервис.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. Выберите вкладку **Транспортные сервисы**.

   По умолчанию выбрана вкладка **X2M-сервисы**, на которой отображается таблица P2M-сервисов и M2M-сервисов.

4. Нажмите на кнопку **+ Транспортный сервис**.

5. В открывшемся окне в поле **Имя** введите имя транспортного P2M-сервиса или M2M-сервиса.

6. В раскрывающемся списке **Тип** выберите тип транспортного сервиса:

   - **P2M**. При выборе этого значения в раскрывающемся списке **Режим** выберите, используется ли в P2M-сервисе DFI (Default Forwarding Interface), на который отправляется неизвестный unicast-трафик:

     - **Классический** – не использовать DFI. Это значение выбрано по умолчанию.

     - **DFI с FIB на root и leafs** – использовать DFI на сервисном интерфейсе с ролью root.

     - **DFI с FIB на leaf** – использовать DFI на сервисном интерфейсе с ролью root. Сервисные интерфейсы с ролью leaf должны быть созданы на одном устройстве CPE. Резервные сервисные интерфейсы с ролью leaf должны быть созданы на одном устройстве CPE, отличном от устройства CPE, на котором созданы основные сервисные интерфейсы.

   - **M2M**.

7. Если вы хотите сделать P2M-сервис или M2M-сервис управляющим, установите флажок **Управляющий транспортный сервис**. Этот флажок снят по умолчанию. Только один транспортный сервис может быть управляющим.

8. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое применяется к серии кадров, когда первый кадр отправляется на контроллер для изучения MAC-адреса источника:

   - **Learn and flood** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отправляется на все добавленные в P2M-сервис сервисные интерфейсы, за исключением сервисного интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.

   - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в MAC-таблице. Если MAC-адрес назначения отсутствует в MAC-таблице, серия кадров отбрасывается.

   При наличии MAC-адреса назначения в MAC-таблице серия кадров отправляется на сервисный интерфейс назначения.

9. В поле **Размер MAC-таблицы** введите максимальное количество записей в MAC-таблице контроллера. Диапазон значений: от 0 до 65 535. Вы можете ввести `0`, чтобы не ограничивать количество записей в MAC-таблице контроллера. Значение по умолчанию: `100`.

10. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. Значение по умолчанию: `300`.

11. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

    - **Flood** – трафик с неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.

    - **Drop** – трафик с неизученными MAC-адресами назначения не передается.

12. Нажмите на кнопку **Создать**.

    P2M-сервис или M2M-сервис будет создан и отобразится в таблице.

13. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Создание L3 VPN-сервиса в шаблоне экземпляра SD-WAN

Чтобы создать L3 VPN-сервис в шаблоне экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN** → **Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, в котором вы хотите создать L3 VPN-сервис.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. Выберите вкладку **Транспортные сервисы** → **L3-сервисы**.

   Отобразится список L3 VPN-сервисов.

4. Нажмите на кнопку **+ Транспортный сервис**.

5. В открывшемся окне введите имя L3 VPN-сервиса.

6. Нажмите на кнопку **Создать**.

   L3 VPN-сервис будет создан и отобразится в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Изменение транспортного сервиса в шаблоне экземпляра SD-WAN

Чтобы изменить транспортный сервис в шаблоне экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN** → **Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, в котором вы хотите изменить транспортный сервис.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. Если вы хотите изменить P2M-сервис или M2M-сервис, выполните следующие действия:

   a. Выберите вкладку **Транспортные сервисы**.

      По умолчанию выбрана вкладка **X2M-сервисы**, на которой отображается таблица P2M-сервисов и M2M-сервисов.

   b. Нажмите на кнопку **Изменить** рядом с P2M-сервисом или M2M-сервисом, который вы хотите изменить.

   c. В открывшемся окне при необходимости измените параметры P2M-сервиса или M2M-сервиса. Описание параметров см. в инструкции со созданию P2M-сервиса или M2M-сервиса в шаблоне экземпляра SD-WAN.

4. Если вы хотите изменить L3 VPN-сервис, выполните следующие действия:

   a. Выберите вкладку **Транспортные сервисы** → **L3-сервисы**.

      Отобразится список L3 VPN-сервисов.

   b. Нажмите на кнопку **Изменить** рядом с L3 VPN-сервисом, который вы хотите изменить.

   c. В открывшемся окне при необходимости измените имя L3 VPN-сервиса.

5. Нажмите на кнопку **Сохранить**.

   Транспортный сервис будет изменен и обновится в таблице.

6. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Удаление транспортного сервиса в шаблоне экземпляра SD-WAN

Удаленные в шаблоне экземпляра SD-WAN транспортные сервисы невозможно восстановить.

Чтобы удалить транспортный сервис в шаблоне экземпляра SD-WAN:

1. В меню перейдите в раздел **SD-WAN** → **Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN, в котором вы хотите удалить транспортный сервис.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. Если вы хотите удалить P2M-сервис или M2M-сервис, выполните следующие действия:

   a. Выберите вкладку **Транспортные сервисы**.

      По умолчанию выбрана вкладка **X2M-сервисы**, на которой отображается таблица P2M-сервисов и M2M-сервисов.

   b. Нажмите на кнопку **Удалить** рядом с P2M-сервисом или M2M-сервисом, который вы хотите удалить.

   P2M-сервис или M2M-сервис будет удален и перестанет отображаться в таблице.

4. Если вы хотите удалить L3 VPN-сервис, выполните следующие действия:

   a. Выберите вкладку **Транспортные сервисы** → **L3-сервисы**.

      Отобразится список L3 VPN-сервисов.

   b. Нажмите на кнопку **Удалить** рядом с L3 VPN-сервисом, который вы хотите удалить.

   L3 VPN-сервис будет удален и перестанет отображаться в таблице.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Работа с транспортными сервисами в шаблоне CPE

Для просмотра таблицы транспортных сервисов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон CPE и выбрать вкладку **Транспортные сервисы**. Информация о транспортных сервисах отображается в следующих столбцах таблицы:

- **Имя** – имя транспортного сервиса.
- **Имя QoS** – имя правила качества обслуживания для сервисного интерфейса, который автоматически создается для подключения устройства CPE к транспортному сервису.
- **Стадия** – состояние, в котором устройство CPE подключается к транспортному сервису:
  - **Перед включением** – устройство CPE подключается к транспортному сервису перед включением этого устройства CPE.
  - **После включения** – устройство CPE подключается к транспортному сервису после включения этого устройства CPE.

  Вы можете выбрать, в каком состоянии устройство CPE находится после регистрации при добавлении устройства CPE.
- **Тип** – тип транспортного сервиса:
  - **P2M**.
  - **M2M**.
  - **L3 VPN**.

- **Параметры соединения** – информация о сервисном интерфейсе, который автоматически создается для подключения устройства CPE к транспортному сервису:
  - Роль сервисного интерфейса:
    - **Leaf**.
    - **Root**.

    Отображается, только если в столбце **Тип** отображается значение **P2M**.
  - Тип классификации трафика на сервисном интерфейсе:
    - **Access**.
    - **VLAN**.
    - **Q-in-Q**.
  - Внешняя метка VLAN сервисного интерфейса. Отображается, только если на сервисном интерфейсе используется тип классификации трафика **VLAN** или **Q-in-Q**.
  - Внутренняя метка VLAN сервисного интерфейса. Отображается, только если на сервисном интерфейсе используется тип классификации трафика **Q-in-Q**.
- **Действия** – действия, которые можно выполнить с транспортным сервисом.

Добавление транспортного сервиса в шаблон CPE

Чтобы добавить транспортный сервис в шаблон CPE:

1. В меню перейдите в подраздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, в который вы хотите добавить транспортный сервис.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Транспортные сервисы**.

   Отобразится таблица транспортных сервисов.

4. Нажмите на кнопку **+ Транспортный сервис**.

5. В открывшемся окне в поле **Имя** введите имя созданного транспортного сервиса. При несовпадении реального имени транспортного сервиса с именем, указанным в шаблоне CPE, устройство CPE не подключается к транспортному сервису.

6. В поле **Имя QoS** введите имя созданного правила качества обслуживания для сервисного интерфейса, который автоматически создается для подключения устройства CPE к транспортному сервису. При несовпадении реального имени правила качества обслуживания с именем, указанным в шаблоне CPE, правило качества обслуживания не применяется к сервисному интерфейсу.

7. В раскрывающемся списке **Стадия** выберите состояние, в котором устройство CPE подключается к транспортному сервису:

   - **Перед включением** – устройство CPE подключается к транспортному сервису перед включением устройства CPE.
   - **После включения** – устройство CPE подключается к транспортному сервису после включения устройства CPE.

   Вы можете выбрать, в каком состоянии устройство CPE находится после регистрации при добавлении или ручной регистрации устройства CPE.

8. В раскрывающемся списке **Тип** выберите тип транспортного сервиса:

   - **P2M**. При выборе этого значения в раскрывающемся списке **Роль** выберите роль сервисного интерфейса, который автоматически создается для подключения устройства CPE к транспортному сервису:
     - **Leaf**.
     - **Root**.
   - **M2M**.
   - **L3 VPN**. При выборе этого значения выполните следующие действия:
     a. В поле **IP-адрес** введите IP-адрес L3-интерфейса.
     b. В поле **Маска** введите длину префикса L3-интерфейса. Диапазон значений: от 0 до 32.

   При несовпадении реального типа транспортного сервиса с типом, указанным в шаблоне CPE, устройство CPE не подключается к транспортному сервису.

9. В раскрывающемся списке **Классификация** выберите тип классификации трафика на сервисном интерфейсе, который автоматически создается для подключения устройства CPE к транспортному сервису:

   - **Access**. Это значение выбрано по умолчанию.
   - **VLAN**. При выборе этого значения в поле **VLAN ID** введите внешнюю метку VLAN сервисного интерфейса. Диапазон значений: от 1 до 4094.
   - **Q-in-Q**. При выборе этого значения настройте L3-интерфейс, который автоматически создается и ссылается на сервисный интерфейс:
     a. В поле **VLAN ID** введите внешнюю метку VLAN сервисного интерфейса. Диапазон значений: от 1 до 4094.
     b. В поле **Внутренний VLAN ID** введите внутреннюю метку VLAN сервисного интерфейса. Диапазон значений: от 1 до 4094.

10. Нажмите на кнопку **Создать**.

    Транспортный сервис будет добавлен и отобразится в таблице.

11. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE.

Изменение транспортного сервиса в шаблоне CPE

Чтобы изменить транспортный сервис в шаблоне CPE:

1. В меню перейдите в подраздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, в котором вы хотите изменить транспортный сервис.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Транспортные сервисы**.

   Отобразится таблица транспортных сервисов.

4. Нажмите на кнопку **Изменить** рядом с транспортным сервисом, который вы хотите изменить.

5. В открывшемся окне при необходимости измените параметры транспортного сервиса. Описание параметров см. в инструкции по добавлению транспортного сервиса в шаблон CPE.

6. Нажмите на кнопку **Сохранить**.

   Транспортный сервис будет изменен и обновится в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE.

Удаление в транспортного сервиса в шаблоне CPE

Удаленные в шаблоне CPE транспортные сервисы невозможно восстановить.

Чтобы удалить транспортный сервис в шаблоне CPE:

1. В меню перейдите в подраздел **SD-WAN → Шаблоны CPE**.

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, в котором вы хотите удалить транспортный сервис.

   Отобразится область настройки параметров. Вы можете развернуть область настройки параметров на всю страницу, нажав на значок развертывания ↙↗. По умолчанию выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Транспортные сервисы**.

   Отобразится таблица транспортных сервисов.

4. Нажмите на кнопку **Удалить** рядом с транспортным сервисом, который вы хотите удалить.

   Транспортный сервис будет удален и перестанет отображаться в таблице.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE.

Зеркалирование и перенаправление трафика между устройствами CPE

Kaspersky SD-WAN поддерживает перенаправление и зеркалирование трафика между устройствами CPE. Вы можете перенаправлять или зеркалировать трафик от точек сбора трафика на точку назначения трафика с помощью TAP-сервисов. При перенаправлении трафик входящий в точки сбора трафика передается на точку назначения трафика, в то время как при зеркалировании передается копия трафика.

В качестве точек сбора и назначения трафика используются сервисные интерфейсы. При этом точками сбора трафика могут быть как отдельные сервисные интерфейсы, так и сервисные интерфейсы, добавленные в транспортный сервис.

Вам нужно создать точку назначения трафика, после чего указать точку назначения трафика и точки сбора трафика при создании или изменении TAP-сервиса. Точки сбора трафика не требуется создавать заранее.

Работа с точками назначения трафика

Для просмотра списка точек назначения трафика вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером и перейти в раздел **TAP-сервисы**.

Действия, которые вы можете выполнить со списком, описаны в инструкции Работа с таблицами компонентов решения.

Создание точки назначения трафика

Чтобы создать точку назначения трафика:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Назначения зеркалирования**, на которой отображается таблица точек назначения трафика.

4. В верхней части страницы нажмите на кнопку **+ Точка назначения**.

5. В открывшемся окне в раскрывающихся списках **Коммутатор** и **Сервисный интерфейс** выберите устройство CPE и созданный сервисный интерфейс, который вы хотите использовать как точку назначения трафика.

6. Нажмите на кнопку **Создать**.

Точка назначения трафика будет создана и отобразится в таблице.

Удаление точки назначения трафика

Удаленные точки назначения трафика невозможно восстановить.

Чтобы удалить точку назначения трафика:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Назначения зеркалирования**, на которой отображается таблица точек назначения трафика.

4. Нажмите на кнопку **Удалить** рядом с точкой назначения трафика, которую вы хотите удалить.

5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Точка назначения трафика будет удалена и перестанет отображаться в таблице.

Работа с TAP-сервисами

Для просмотра таблицы TAP-сервисов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Параметры развертывания** рядом с контроллером, перейти в раздел **TAP-сервисы** и выбрать вкладку **TAP-сервисы**. Информация о TAP-сервисах отображается в следующих столбцах таблицы:

- **Точка назначения** – информация о сервисном интерфейсе, который используется как точка назначения трафика:
  - имя и идентификатор DPID устройства CPE, на котором создан сервисный интерфейс;
  - номер OpenFlow-порта, на который ссылается сервисный интерфейс.
- **Зеркалировать** – TAP-сервис зеркалирует трафик от точек сборка трафика на точку назначения трафика:
  - **Да**.
  - **Нет**.
- **Тип** – тип точек сбора трафика:
  - **SI** – в качестве точек сбора трафика используются отдельные сервисные интерфейсы.
  - Если в качестве точек сбора трафика используются сервисные интерфейсы, добавленные в транспортный сервис, отображается тип транспортного сервиса:
    - **P2P**.
    - **IP multicast**.
    - **L3 VPN**.
    - **P2M**.
    - **M2M**.
- **Транспортный сервис** – транспортный сервис, в который добавлены сервисные интерфейсы, используемые как точки сборка трафика. Значение в этом столбце отображается, только если в столбце **Тип точки сбора** отображается тип транспортного сервиса.
- **Точки сбора** – информация о сервисных интерфейсах, которые используются как точки сбора трафика:
  - имена и идентификаторы DPID устройств CPE, на которых созданы сервисные интерфейсы;
  - номера OpenFlow-портов, на которые ссылаются сервисные интерфейсы.
- **Статус** – статус TAP-сервиса:
  - **Работает**.
  - **Не работает**.

Действия, которые вы можете выполнить с таблицей, описаны в статье Работа с таблицами компонентов решения.

Создание TAP-сервиса

Чтобы создать TAP-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Назначения зеркалирования**, на которой отображается таблица точек назначения трафика.

4. Выберите вкладку **TAP-сервисы**.

   Отобразится таблица TAP-сервисов.

5. В верхней части страницы нажмите на кнопку **+ TAP-сервис**.

6. Если вы хотите, чтобы TAP-сервис зеркалировал трафик от точек сборка трафика на точку назначения трафика, установите флажок **Зеркалировать**. Когда флажок установлен, на точку назначения трафика передается копия трафика, а когда снят – трафик перенаправляется. Этот флажок снят по умолчанию.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для распределения трафика по соединениям:

   - **По потокам** – потоки трафика (5-Tuple) распределяются по соединениям в соответствии со стоимостью соединений. Это значение выбрано по умолчанию.
   - **По пакетам** – пакеты трафика распределяются по соединениям в соответствии со стоимостью соединений.
   - **Широковещательный** – пакеты трафика дублируются и передаются одновременно через все соединения для исключения потерь.

   Вы можете указать стоимость соединения вручную.

8. При необходимости настройте режим адаптивной балансировки, если хотите, чтобы вес пути динамически корректировался в зависимости от уровня пакетных потерь на пути:

   a. Включите переключатель **Включить адаптивную балансировку**.

   b. В поле **Минимальный уровень потерь (%)** укажите минимальный процент пакетных потерь на пути, при котором режим адаптивной балансировки начинает влиять на вес. Диапазон значений: 0.01 – 100.

   c. В поле **Максимальный уровень потерь (%)** укажите максимальный процент пакетных потерь, при котором путь исключается из балансировки нагрузки.

   d. В раскрывающемся списке **Скорость схождения** выберите скорость схождения адаптивных весов к расчетным значениям:

      - **Fast** – 1;
      - **Fast** – 0,75;
      - **Fast** – 0,5.

9. В раскрывающемся списке **Точка назначения** выберите созданную точку назначения трафика.

10. В раскрывающемся списке **Тип точки сбора** выберите тип точек сбора трафика:

    - **Сервисный интерфейс** – в качестве точек сбора трафика используются отдельные сервисные интерфейсы.
    - **Транспортный сервис** – в качестве точек сбора трафика используются сервисные интерфейсы, добавленные в транспортный сервис.

11. Если в раскрывающемся списке **Тип точки сбора** вы выбрали **Транспортный сервис**, выполните следующие действия:

    a. В раскрывающемся списке **Тип** выберите тип транспортного сервиса:

       - **P2P**.
       - **IP multicast**.
       - **L3 VPN**.
       - **P2M**.
       - **M2M**.

    b. В раскрывающемся списке **Транспортный сервис** выберите транспортный сервис.

12. В раскрывающемся списке **Точки сбора** выберите созданный сервисный интерфейс, который вы хотите использовать как точку сбора трафика.

    Точка сбора трафика будет добавлена и отобразится в нижней части окна. Вы можете добавить несколько точек сбора трафика и удалить точки сбора трафика. Для удаления точки сбора трафика нажмите рядом с ней на кнопку **Удалить**.

13. Нажмите на кнопку **Далее** и выберите созданные правила классификации трафика для точек сборка трафика.

14. Нажмите на кнопку **Создать**.

TAP-сервис будет создан и отобразится в таблице.

Просмотр статистики работы TAP-сервиса

Чтобы посмотреть статистику работы TAP-сервиса:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Назначения зеркалирования**, на которой отображается таблица точек назначения трафика.

4. Выберите вкладку **TAP-сервисы**.

   Отобразится таблица TAP-сервисов.

5. Нажмите на кнопку **Управление** → **Статистика** рядом с TAP-сервисом, статистику работы которого вы хотите посмотреть.

Откроется окно со статистикой работы TAP-сервиса.

Изменение TAP-сервиса

Чтобы изменить TAP-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Назначения зеркалирования**, на которой отображается таблица точек назначения трафика.

4. Выберите вкладку **TAP-сервисы**.

   Отобразится таблица TAP-сервисов.

5. Нажмите на кнопку **Управление** → **Изменить** рядом с TAP-сервисом, который вы хотите изменить.

6. В открывшемся окне при необходимости измените параметры TAP-сервиса. Описание параметров см. в инструкции по созданию TAP-сервиса.

7. Нажмите на кнопку **Сохранить**.

TAP-сервис будет изменен и обновится в таблице.

Удаление TAP-сервиса

Удаленные TAP-сервисы невозможно восстановить.

Чтобы удалить TAP-сервис:

1. В меню перейдите в раздел **Инфраструктура**.

   Откроется страница управления ресурсами. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров.

2. Нажмите на имя контроллера или выберите контроллер в таблице и нажмите **Параметры развертывания.**

   Откроется меню настройки параметров развертывания контроллера. По умолчанию вы переходите в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Назначения зеркалирования**, на которой отображается таблица точек назначения трафика.

4. Выберите вкладку **TAP-сервисы**.

   Отобразится таблица TAP-сервисов.

5. Нажмите на кнопку **Управление** → **Удалить** рядом с TAP-сервисом, который вы хотите удалить.

6. Если вы хотите удалить добавленные в TAP-сервис сервисные интерфейсы, в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**. Этот флажок снят по умолчанию.

7. Нажмите на кнопку **Удалить**.

TAP-сервис будет удален и перестанет отображаться в таблице.

Интеграция с Kaspersky Unified Monitoring and Analysis Platform

Вы можете использовать Kaspersky Unified Monitoring and Analysis Platform (далее также KUMA) для получения уведомлений о событиях безопасности, произошедших на оркестраторе и устройствах CPE. В этом разделе описаны шаги по установке и настройке KUMA.

> Kaspersky SD-WAN не выполняет функции агента для KUMA, а только отправляет в KUMA события без разметки.

Для установки KUMA вам потребуется образ операционной системы Astra Linux 1.8.5. Список операционных систем, поддерживаемых KUMA, см. в справке KUMA.

Установка KUMA

Чтобы установить KUMA:

1. Настройте имя хоста на сервере, на котором вы хотите установить KUMA:

   ```
   sudo hostnamectl set-hostname kuma.local
   ```

2. Проверьте, что на хосте присутствует список DNS-серверов, в случае необходимости заполните его:

   ```
   cat /etc/resolv.conf
   ```

3. На сервере, на котором вы хотите установить KUMA, укажите IP-адрес сервера в формате `<IP-адрес> kuma.local` в файле для сопоставления IP-адресов с доменными именами:

   ```
   vi /etc/hosts
   ```

4. Установите необходимые пакеты:

   ```
   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. Если на сервере используется механизм SELINUX, отключите его, установив `SELINUX=disabled`:

   ```
   vi /etc/selinux/config
   ```

6. Активируйте синхронизацию времени и проверьте ее работу:

```
sudo systemctl enable --now chronyd sudo timedatectl | grep 'System clock synchronized'
```

7. Если для входа на сервер вы хотите использовать учетную запись root, укажите `PermitRootLogin yes` в файле конфигурации SSH:

```
vi /etc/ssh/sshd_config
```

8. Перезагрузите сервер.

9. Скопируйте архив с установщиком `kuma-ansible-installer-<номер версии>.tar.gz` на сервер и распакуйте его с помощью команды ниже. Для распаковки архива потребуется около 2 ГБ дискового пространства.

```
sudo tar -xpf kuma-ansible-installer-<номер версии>.tar.gz
```

10. Перейдите в директорию установщика:

```
cd kuma-ansible-installer
```

11. Скопируйте шаблон `single.inventory.yml.template` и создайте на его основе файл инвентаря с именем `single.inventory.yml`:

```
cp single.inventory.yml.template single.inventory.yml
```

12. Откройте файл `single.inventory.yml` для редактирования:

```
vi single.inventory.yml
```

13. Измените содержимое файла по аналогии с примером ниже:

```
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. Подготовьте файл ключа KUMA.

15. Скопируйте файл ключа в директорию:

```
sudo cp <файл ключа>.key <директория установщика>/roles/kuma/files/license.key
```

16. Запустите установщик:

```
sudo ./install.sh single.inventory.yml
```

Дождитесь окончания установки KUMA.

17. Выполните вход в веб-интерфейс KUMA:

a. Перейдите в браузере по адресу `https://<FQDN хоста, на котором установлена KUMA>:7220`

b. Введите учетные данные для входа по умолчанию:

- логин – `admin`
- пароль – `mustB3Ch@ng3d!`

18. Измените пароль учетной записи admin.

Более подробную информацию по установке KUMA см. в справке KUMA.

Сценарий: настройка KUMA

В этом сценарии описана процедура настройки Kaspersky Unified Monitoring and Analysis Platform для интеграции с Kaspersky SD-WAN.

Настройка KUMA состоит из следующих этапов:

1. **Вход в веб-интерфейс KUMA**

   Выполните вход в веб-интерфейс KUMA, если еще не сделали это. Убедитесь, что изменили пароль по умолчанию.

2. Настройка хранилища
3. Создание и настройка нормализатора для syslog-событий
4. Настройка коррелятора и правил корреляции
5. Настройка коллектора для syslog-событий
6. Настройка почтовой службы
7. Настройка правил уведомления

Более подробную информацию по настройке KUMA см. в справке KUMA.

Настройка хранилища в KUMA

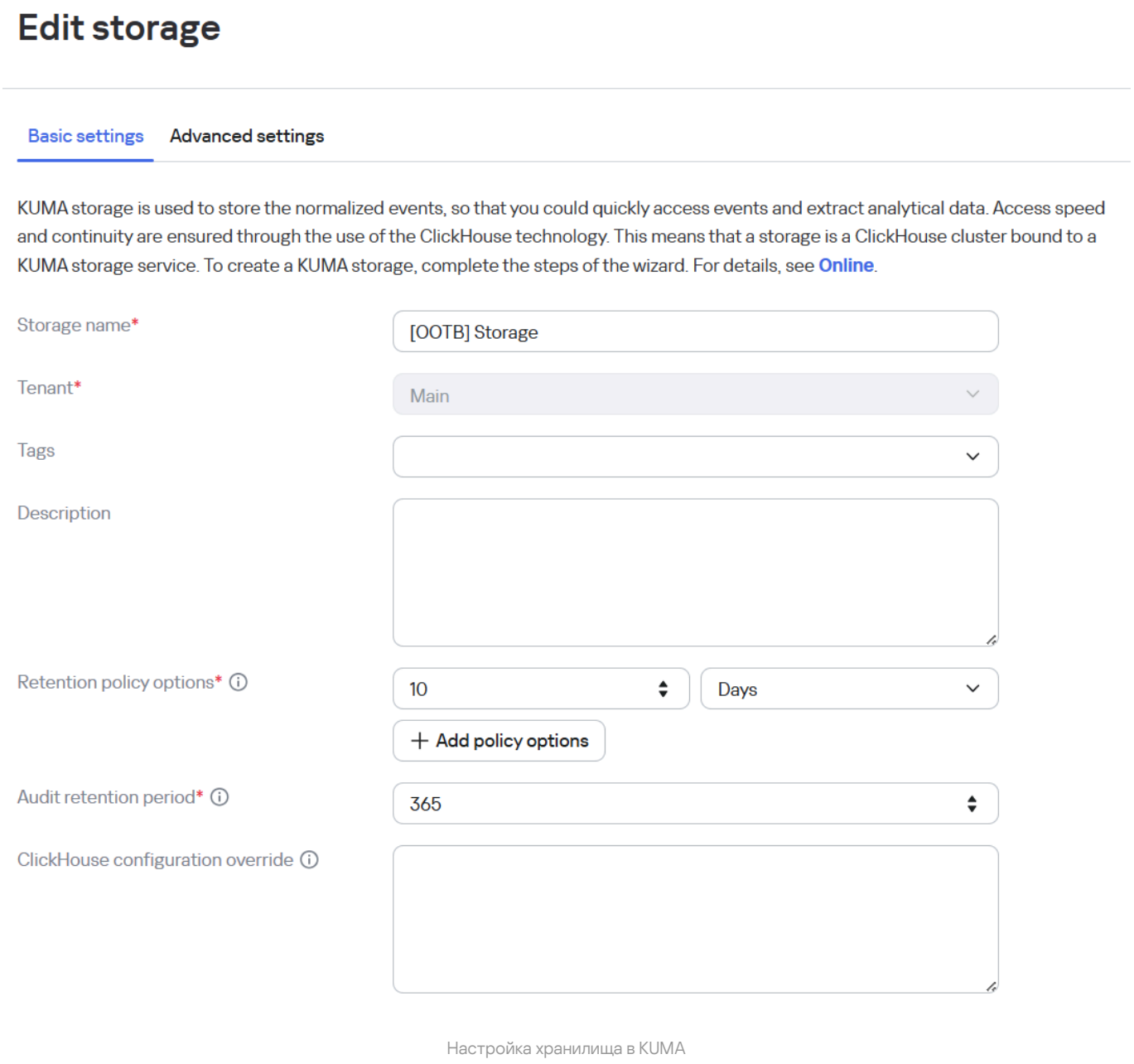
По умолчанию для хранилища `[00TB] Storage` настроено хранение событий не более 2 дней, после чего события удаляются.

Чтобы увеличить количество дней хранения событий:

1. Перейдите в раздел **Resources** → **Storages**.
2. Откройте созданное по умолчанию хранилище `[00TB] Storage`.
3. Перейдите на вкладку **Basic settings**.

4. Измените параметр **Retention policy options**.

   Вы можете указать значение в днях, гигабайтах или процентах. Установите значение, определенное политикой безопасности в вашей компании (например, 10 дней).



Настройка хранилища в KUMA

5. Сохраните изменения с помощью кнопки **Save**.

6. Чтобы изменения применились, обновите параметры сервиса:

   a. Перейдите в раздел **Resources** → **Active services**.

      Сервис хранилища `[OOTB] Storage` будет отображаться в списке со статусом **Update required**.

   b. Установите флажок рядом с сервисом хранилища `[OOTB] Storage` и нажмите **Update configuration**.

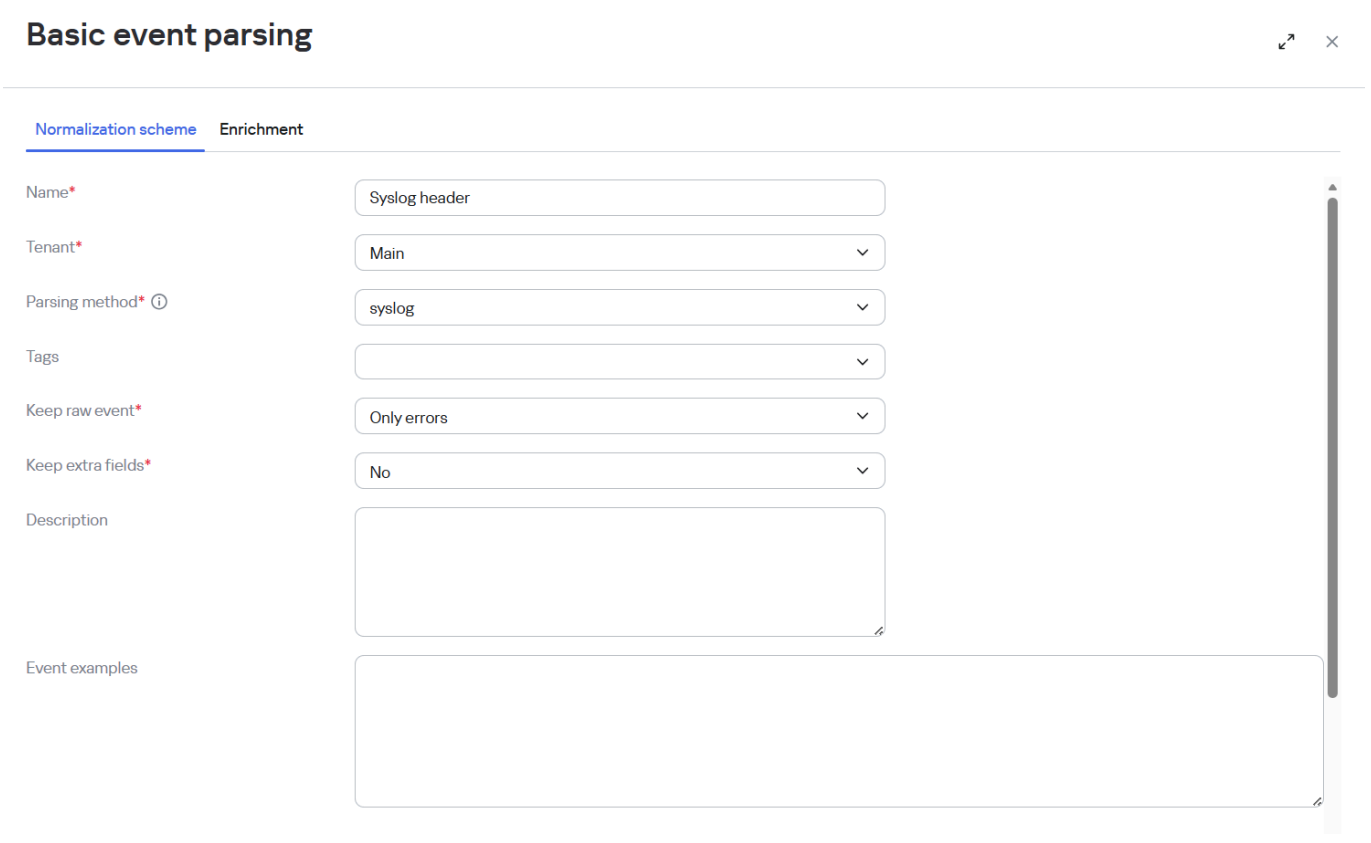
Параметры сервиса будут обновлены без перезапуска, и изменения вступят в силу.

Создание и настройка нормализатора в KUMA для syslog-событий

Для получения syslog-сообщений от оркестратора SD-WAN и CPE и приведения их к модели данных KUMA необходимо создать нормализатор.

Чтобы создать нормализатор:

1. Перейдите в раздел **Resources** → **Normalizer**.
2. Нажмите **+Create**.
3. Заполните поля на вкладке **Normalization scheme**:
   - В поле **Name** укажите название нормализатора, например, `Syslog header`.
   - В поле **Tenant** выберите `Main`.
   - В поле **Parsing method** выберите `syslog`.
   - В поле **Keep raw event** выберите `Only errors`.
   - В поле **Keep extra fields** выберите `No`.

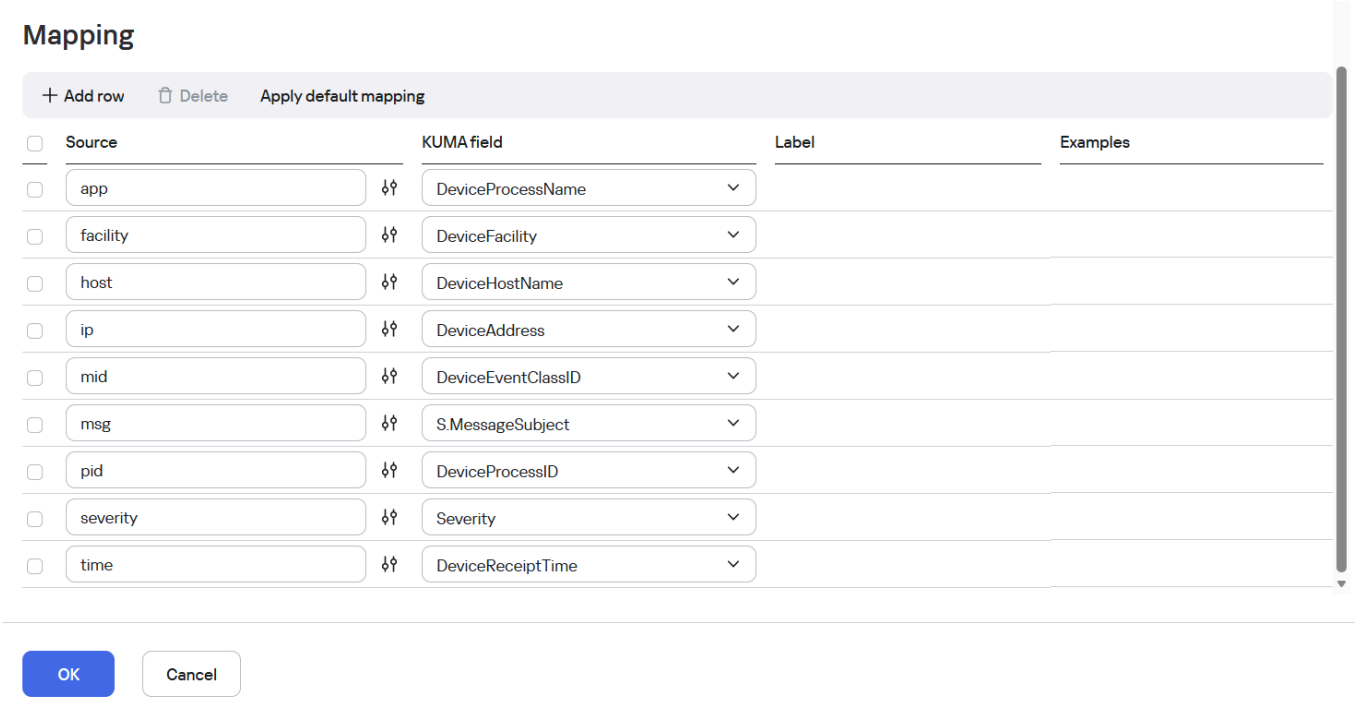


Настройка основных параметров нормализатора в KUMA

4. Настройте сопоставление полей:

   a. На вкладке **Normalization scheme** перейдите в блок **Mapping** и нажмите **Apply default mapping**.

   b. Для значения `msg` в поле **Source** измените значение в поле **KUMA field** на `S.MessageSubject` (поддерживает больше символов, чем стандартное значение 1024).



Настройка сопоставления полей в KUMA

   a. Нажмите **OK**.

5. Нажмите **Create new**.

Изменения будут сохранены.

Настройка коррелятора и правил корреляции в KUMA

Для получения в KUMA alert-уведомлений о событиях безопасности от оркестратора SD-WAN и CPE необходимо выполнить настройку коррелятора и правил корреляции.

Коррелятор – это сервис, который анализирует события, получаемые от сервиса коллектора (Syslog) по параметрам, настроенным в правилах корреляции, и выполняет уведомление о событии.

Правило корреляции – это правило, в котором описывается признак срабатывания и назначаемый уровень критичности.

Настройка правил корреляции

Чтобы настроить правила корреляции:

1. Перейдите в раздел **Resources** → **Correlation rules**.

2. Нажмите **+Create**.

3. В отобразившемся окне заполните параметры правила корреляции в соответствии с таблицей.

4. Перейдите на вкладку **Actions** и активируйте правило с помощью output.

5. Повторите действия для остальных правил корреляции.

Изменения будут сохранены.

Настройка коррелятора

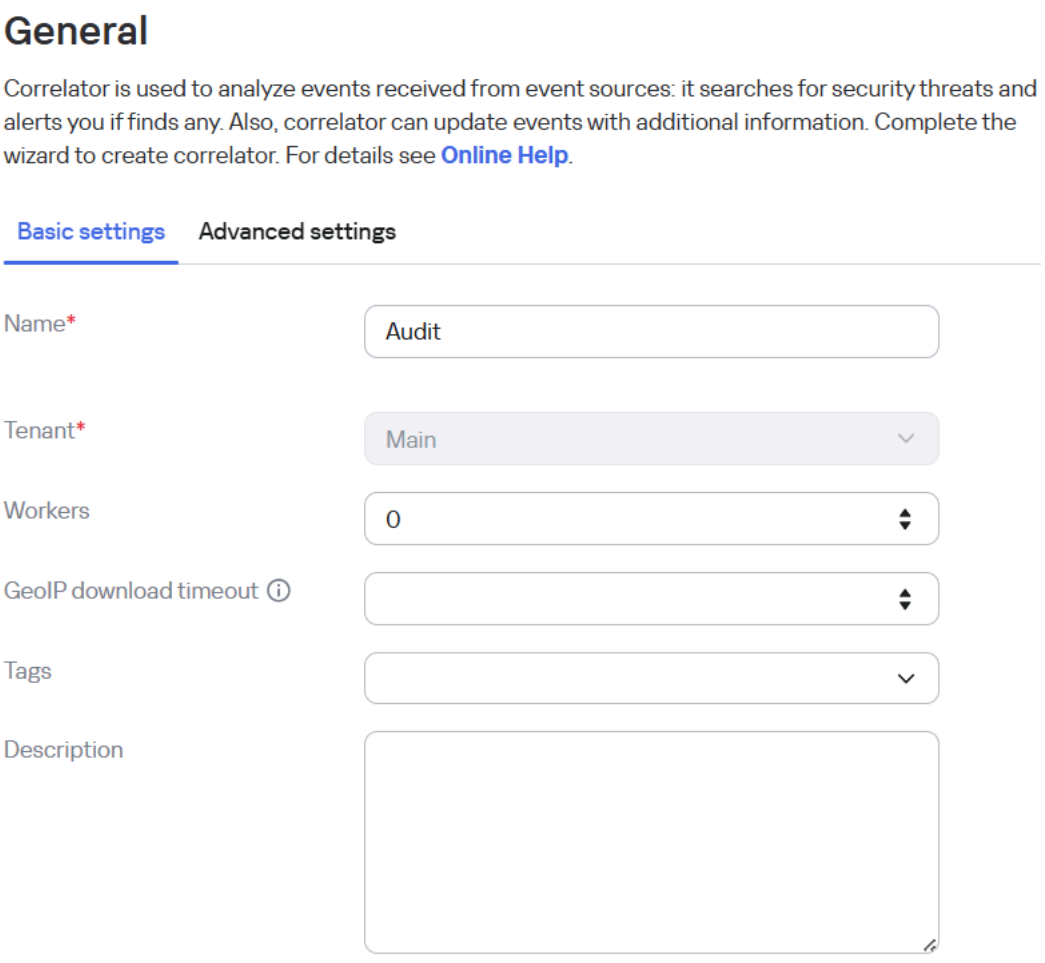
Чтобы настроить коррелятор:

1. Перейдите в раздел **Resources** → **Correlators**.

2. Нажмите **+Create**.

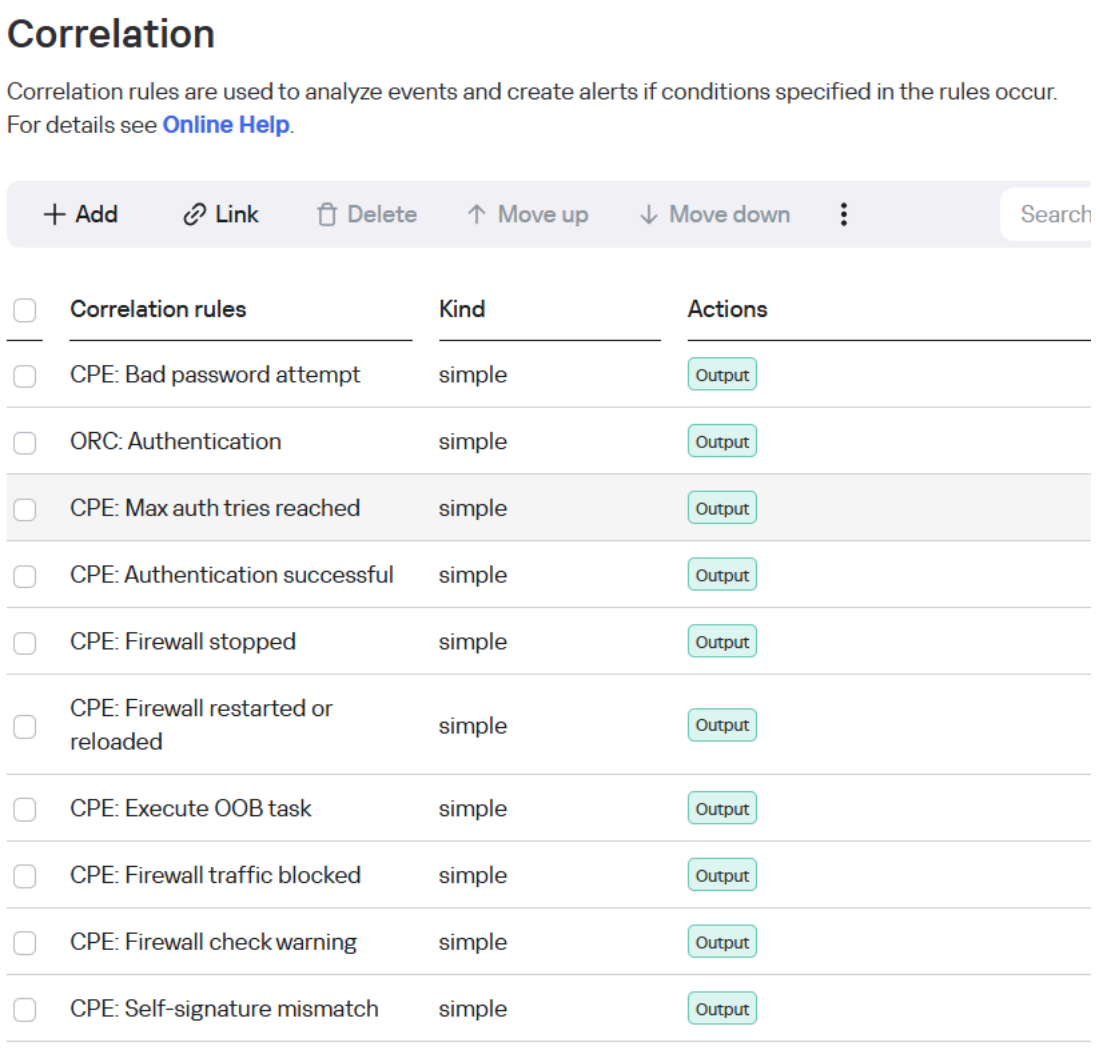
3. На вкладке **General** заполните поля:

   - **Name** – название коррелятора (например, `Audit`).
   - **Tenant** – `Main` (выберите другой, если требуется).



Параметры коррелятора на вкладке **General** в KUMA

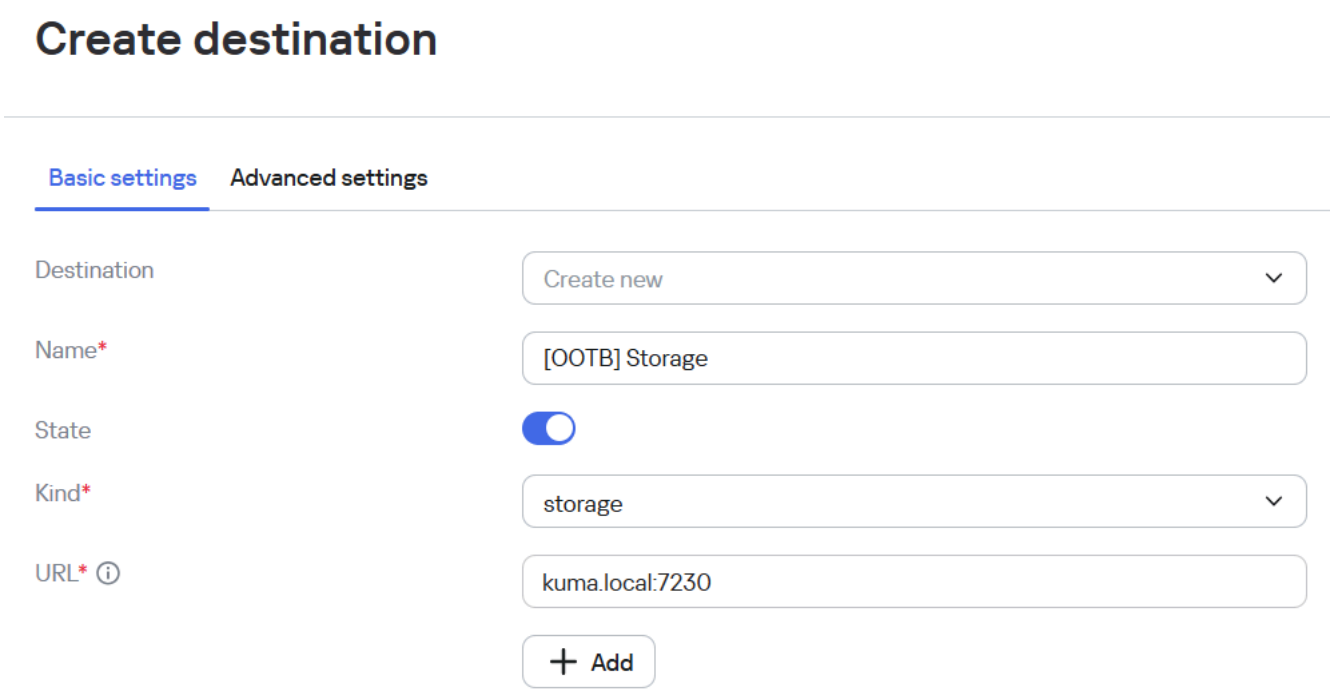
4. На вкладке **Correlation** нажмите **Link** и в открывшемся окне выберите из списка все ранее созданные правила корреляции.



Настройка правил корреляции в коррелляторе в KUMA

5. На вкладке **Routing** нажмите **+Add** и заполните поля:

   - **Kind** – выберите `storage`. После этого появится поле **URL**.
   - **URL** – выберите доступный [OOTB] Storage (выберите другой, если требуется).
   - **Name** – автоматически будет заполнено после выбора в поле **URL**.



Параметры коррелятора на вкладке **Routing** в KUMA

6. На вкладке **Setup validation** нажмите **Create and save service** и получите команду запуска, которую необходимо выполнить через CLI на сервере KUMA.

7. Нажмите **Save**.

Изменения будут сохранены.

Справочная таблица для создания правил корреляции KUMA

Название	Тип	Наследуемые поля	Уровень важности	Селекторы	Действия	Коррелятор
ORC: Audit started	simple	Message	Низкий	Message contain SYS-AUD Started:	В дальнейшую обработку	Audit
ORC: Audit stopped	simple	Message	Средний	Message contain SYS-AUD Stopped:	В дальнейшую обработку	Audit
ORC: CPE Change	simple	Message	Низкий	Message contain SDW-CPE Any:	В дальнейшую обработку	Audit
ORC: CPE Change Error	simple	Message	Средний	Message contain SDW-CPE AnyError:	В дальнейшую обработку	Audit
ORC: CPE Create	simple	Message	Низкий	Message contain SDW-CPE Create:	В дальнейшую обработку	Audit
ORC: CPE Create Error	simple	Message	Средний	Message contain SDW-CPE CreateError:	В дальнейшую обработку	Audit

Название	Тип	Наследуемые поля	Уровень важности	Селекторы	Действия	Коррелятор
ORC: CPE Registration	simple	Message	Низкий	Message contain SDW-CPE Registration:	В дальнейшую обработку	Audit
ORC: CPE Registration Error	simple	Message	Средний	Message contain SDW-CPE RegistrationError:	В дальнейшую обработку	Audit
ORC: CPE Delete	simple	Message	Низкий	Message contain SDW-CPE Delete:	В дальнейшую обработку	Audit
ORC: CPE Delete Error	simple	Message	Средний	Message contain SDW-CPE DeleteError:	В дальнейшую обработку	Audit
ORC: CPE Disable	simple	Message	Низкий	Message contain SDW-CPE Disable:	В дальнейшую обработку	Audit
ORC: CPE Disable Error	simple	Message	Средний	Message contain SDW-CPE DisableError:	В дальнейшую обработку	Audit
ORC: CPE Enable	simple	Message	Низкий	Message contain SDW-CPE Enable:	В дальнейшую обработку	Audit
ORC: CPE Enable Error	simple	Message	Средний	Message contain SDW-CPE EnableError:	В дальнейшую обработку	Audit
ORC: CPE Firewall Template	simple	Message	Низкий	Message contain SDW-CPE-GEN FirewallTemplate:	В дальнейшую обработку	Audit
ORC: CPE Firewall Template Error	simple	Message	Средний	Message contain SDW-CPE-GEN FirewallTemplateError:	В дальнейшую обработку	Audit
ORC: CPE Encryption	simple	Message	Низкий	Message contain SDW-CPE-ENC Encryption:	В дальнейшую обработку	Audit
ORC: CPE Encryption Error	simple	Message	Средний	Message contain SDW-CPE-ENC EncryptionError:	В дальнейшую обработку	Audit
ORC: CPE Scripts	simple	Message	Низкий	Message contain SDW-CPE-SCR Scripts:	В дальнейшую обработку	Audit
ORC: CPE Scripts Error	simple	Message	Средний	Message contain SDW-CPE-SCR ScriptsError:	В дальнейшую обработку	Audit
ORC: CPE Interface	simple	Message	Низкий	Message contain SDW-CPE-NET Interface:	В дальнейшую обработку	Audit
ORC: CPE Interface Error	simple	Message	Средний	Message contain SDW-CPE-NET InterfaceError:	В дальнейшую обработку	Audit
ORC: CPE Firewall	simple	Message	Низкий	Message contain SDW-CPE-FW Firewall:	В дальнейшую обработку	Audit
ORC: CPE Firewall Error	simple	Message	Средний	Message contain SDW-CPE-FW FirewallError:	В дальнейшую обработку	Audit
ORC: CPE Static Route	simple	Message	Низкий	Message contain SDW-CPE-STR StaticRoute:	В дальнейшую обработку	Audit
ORC: CPE Static Route Error	simple	Message	Средний	Message contain SDW-CPE-STR StaticRouteError:	В дальнейшую обработку	Audit
ORC: CPE Template Change	simple	Message	Низкий	Message contain SDW-CPET Any:	В дальнейшую обработку	Audit
ORC: CPE Template Change Error	simple	Message	Средний	Message contain SDW-CPET AnyError:	В дальнейшую обработку	Audit
ORC: CPE Template Encryption	simple	Message	Низкий	Message contain SDW-CPET-ENC Encryption:	В дальнейшую обработку	Audit
ORC: CPE Template Encryption Error	simple	Message	Средний	Message contain SDW-CPET-ENC EncryptionError:	В дальнейшую обработку	Audit
ORC: CPE Template Scripts	simple	Message	Низкий	Message contain SDW-CPET-SCR Scripts:	В дальнейшую обработку	Audit
ORC: CPE Template Scripts Error	simple	Message	Средний	Message contain SDW-CPET-SCR ScriptsError:	В дальнейшую обработку	Audit

Название	Тип	Наследуемые поля	Уровень важности	Селекторы	Действия	Коррелятор
ORC: CPE Template Interface	simple	Message	Низкий	Message contain SDW-CPET-NET Interface:	В дальнейшую обработку	Audit
ORC: CPE Template Interface Error	simple	Message	Средний	Message contain SDW-CPET-NET InterfaceError:	В дальнейшую обработку	Audit
ORC: CPE Template Static Route	simple	Message	Низкий	Message contain SDW-CPET-STR StaticRoute:	В дальнейшую обработку	Audit
ORC: CPE Template Static Route Error	simple	Message	Средний	Message contain SDW-CPET-STR StaticRouteError:	В дальнейшую обработку	Audit
ORC: Firewall Template	simple	Message	Низкий	Message contain SDW-FWT Firewall:	В дальнейшую обработку	Audit
ORC: Firewall Template Error	simple	Message	Средний	Message contain SDW-FWT FirewallError:	В дальнейшую обработку	Audit
ORC: Zone Template	simple	Message	Низкий	Message contain SDW-FWZ Zone:	В дальнейшую обработку	Audit
ORC: Zone Template Error	simple	Message	Средний	Message contain SDW-FWZ ZoneError:	В дальнейшую обработку	Audit
ORC: Firmware	simple	Message	Низкий	Message contain SDW-FMW Firmware:	В дальнейшую обработку	Audit
ORC: Firmware Error	simple	Message	Средний	Message contain SDW-FMW FirmwareError:	В дальнейшую обработку	Audit
ORC: Firmware Update	simple	Message	Низкий	Message contain SCH-FMWU FirmwareUpdate:	В дальнейшую обработку	Audit
ORC: Firmware Update Error	simple	Message	Средний	Message contain SCH-FMWU FirmwareUpdateError:	В дальнейшую обработку	Audit
ORC: Scheduled Update Settings	simple	Message	Низкий	Message contain SCH-UPDS UpdateSettings:	В дальнейшую обработку	Audit
ORC: Scheduled Update Settings Error	simple	Message	Средний	Message contain SCH-UPDS UpdateSettingsError:	В дальнейшую обработку	Audit
ORC: User Authentication	simple	Message	Низкий	Message contain USR-USR Authentication:	В дальнейшую обработку	Audit
ORC: User Authentication Error	simple	Message	Средний	Message contain USR-USR AuthenticationError:	В дальнейшую обработку	Audit
ORC: User Change	simple	Message	Низкий	Message contain USR-USR UserChange:	В дальнейшую обработку	Audit
ORC: User Permission	simple	Message	Низкий	Message contain USR-PERM UserPermissions:	В дальнейшую обработку	Audit
ORC: API Call	simple	Message	Низкий	Message contain SYS-API Call:	В дальнейшую обработку	Audit
ORC: API Call Complete	simple	Message	Низкий	Message contain SYS-API CallComplete:	В дальнейшую обработку	Audit
CPE: Authentication successful	simple	Message	Низкий	DeviceFacility = 10, Severity = 5, Message contains Password auth succeeded	В дальнейшую обработку	Audit
CPE: Max auth tries reached	simple	Message	Высокий	DeviceFacility = 10, Severity = 6, Message contains Max auth tries reached	В дальнейшую обработку	Audit
CPE: Bad password attempt	simple	Message	Средний	DeviceFacility = 10 Severity = 4 Message contains Bad password attempt	В дальнейшую обработку	Audit
CPE: Execute OOB task	simple	Message	Низкий	DeviceFacility = 1, Severity = 6, Message contains sdwan-oob:	В дальнейшую обработку	Audit

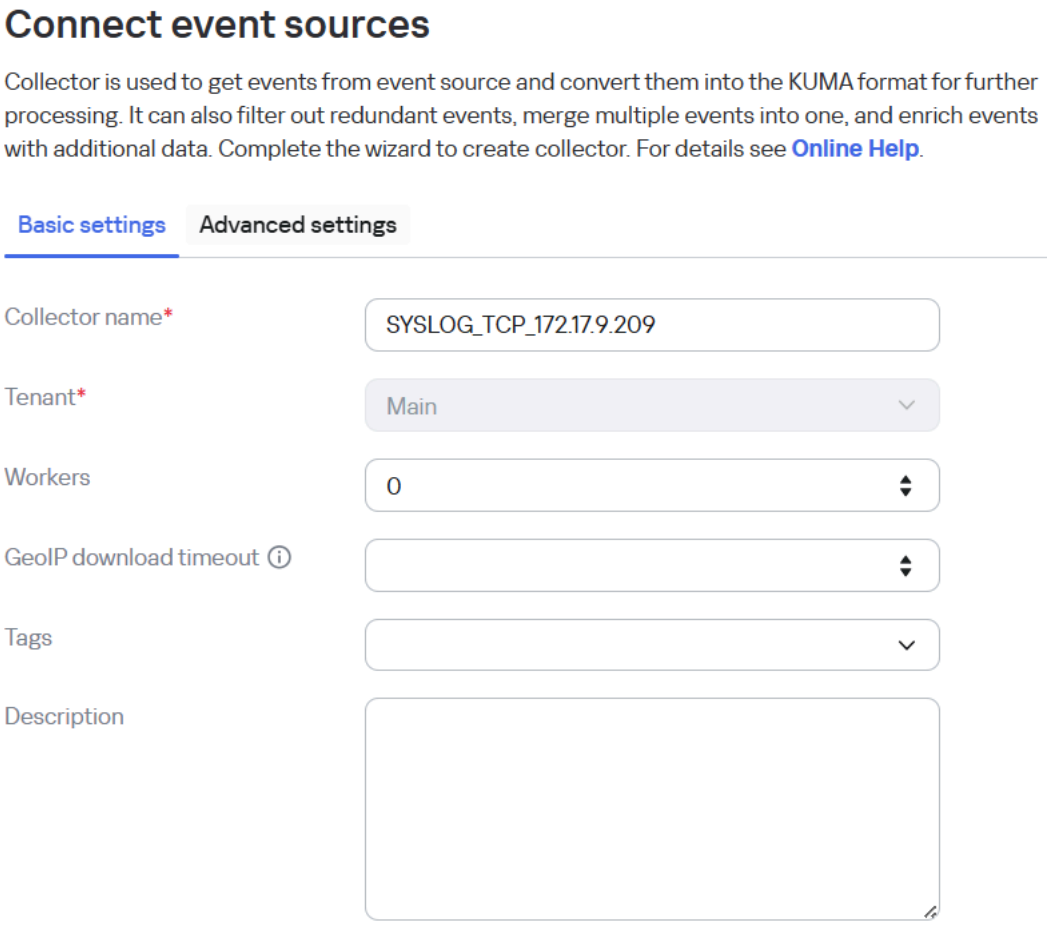
Название	Тип	Наследуемые поля	Уровень важности	Селекторы	Действия	Коррелятор
CPE: Firewall stopped	simple	Message	Критический	DeviceFacility = 1, Severity = 2, Message contains Firewall stopped	В дальнейшую обработку	Audit
CPE: Firewall started	simple	Message	Низкий	DeviceFacility = 1, Severity = 6, Message contains Firewall started	В дальнейшую обработку	Audit
CPE: Firewall restarted or reloaded	simple	Message	Средний	DeviceFacility = 1, Severity = 4, OR Message contains Firewall reloaded Message contains Firewall restarted	В дальнейшую обработку	Audit
CPE: Firewall audit	simple	Message	Низкий	DeviceFacility = 0, Severity = 6, Message contains FW-AUD	В дальнейшую обработку	Audit
CPE: Integrity check successful	simple	Message	Низкий	DeviceFacility = 1, Severity = 6, Message contains Integrity check successful	В дальнейшую обработку	Audit
CPE: Integrity check failed	simple	Message	Критический	DeviceFacility = 1, Severity = 2, Message endsWith Integrity check failed	В дальнейшую обработку	Audit
CPE: Verification mismatch	simple	Message	Критический	DeviceFacility = 1, Severity = 2, Message contains Verification mismatch	В дальнейшую обработку	Audit
CPE: Firewall traffic blocked	simple	Message	Критический	DeviceFacility = 1, Severity = 2,Message contains Integrity check failed. Traffic forwarding blocked	В дальнейшую обработку	Audit
CPE: Firewall self-test successful	simple	Message	Низкий	DeviceFacility = 1, Severity = 6, Message contains Successful firewall self test	В дальнейшую обработку	Audit
CPE: Firewall self-test failed	simple	Message	Критический	DeviceFacility = 1, Severity = 2, Message contains Firewall self test failed	В дальнейшую обработку	Audit
CPE: USB device inserted	simple	Message	Средний	DeviceFacility = 0, Severity = 6, OR Message contains USB deviceMessage contains Storage device detected	В дальнейшую обработку	Audit
CPE: USB device mounted	simple	Message	Высокий	DeviceFacility = 0, Severity = 6, Message contains mounted filesystem	В дальнейшую обработку	Audit
CPE: Time jump detected	simple	Message	Средний	DeviceFacility = 3, Severity = 4, Message contains time jump detected	В дальнейшую обработку	Audit

Настройка коллектора для syslog-событий в KUMA

Для получения syslog-сообщений с оркестратора SD-WAN и устройств CPE необходимо создать коллектор KUMA.

Чтобы настроить коллектор KUMA:

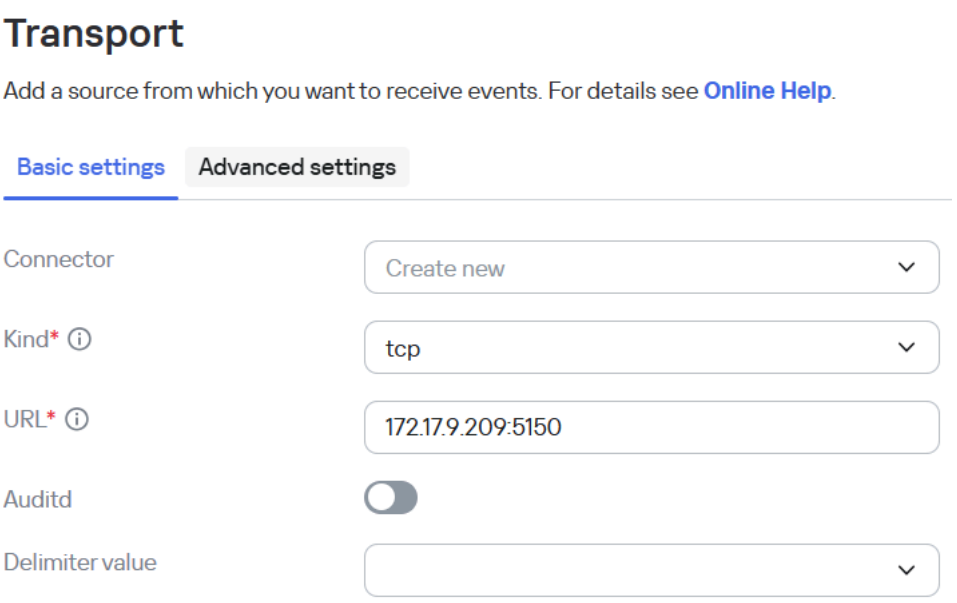
1. Перейдите в раздел **Resources** → **Collectors**.
2. Нажмите **+Create**.
3. На вкладке **Connect event sources** → **Basic settings** заполните поля:
   - **Collector name** – название коллектора (например, `SYSLOG_TCP_172.17.9.209`).
   - **Tenant** – `Main` (выберите другой, если требуется).



Параметры коллектора на вкладке **Connect event sources** → **Basic settings** в KUMA

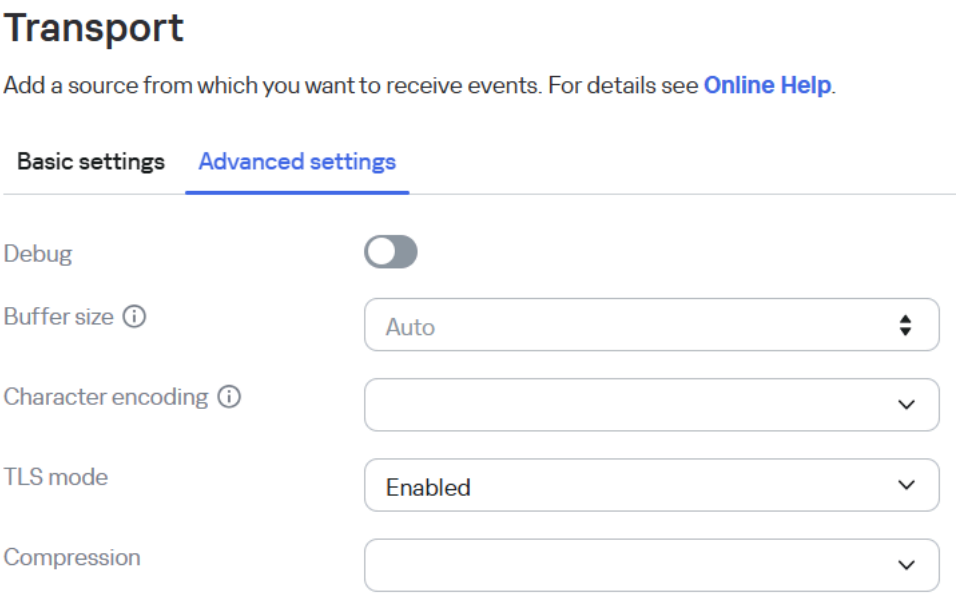
4. На вкладке **Transport** → **Basic settings** заполните поля:

   - **Kind** – `tcp`.
   - **URL** – `<IP-адрес>:<порт>` (например, 172.17.9.209:5150).



Параметры коллектора на вкладке **Transport** → **Basic settings** в KUMA

5. На вкладке **Transport** → **Advanced settings** в поле **TLS mode** выберите **Enabled**.

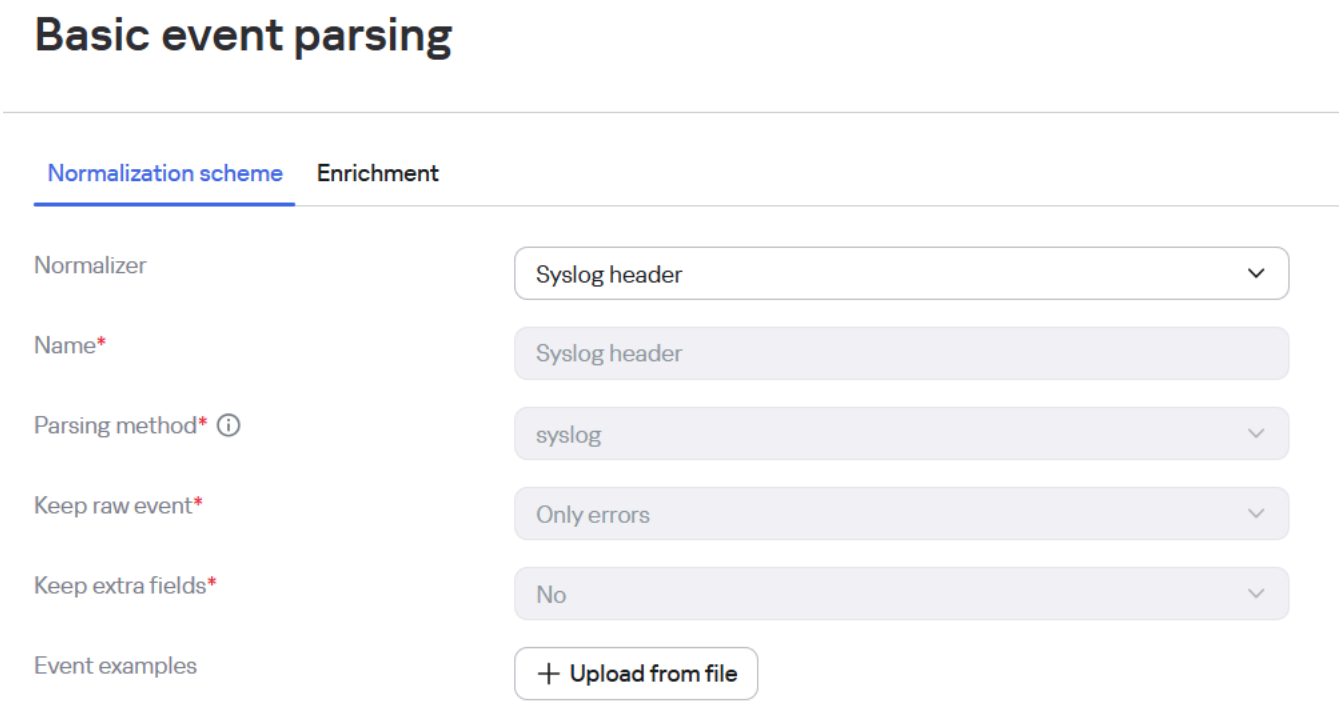


Параметры коллектора на вкладке **Transport** → **Advanced settings** в KUMA

6. На вкладке **Event parsing** нажмите **+Add event parsing** и в поле **Normalizer** выберите созданный ранее шаблон `Syslog header`.

   Все остальные поля автоматически заполнятся.

7. Нажмите **OK**.



Параметры коллектора на вкладке **Event parsing** в KUMA

8. На вкладке **Routing** нажмите **+Add** и заполните поля:

- **Kind** – выберите `storage`. После этого появится поле **URL**.
- **URL** – выберите доступный [OOTB] Storage (выберите другой, если требуется).
- **Name** – автоматически будет заполнено после выбора в поле **URL**.

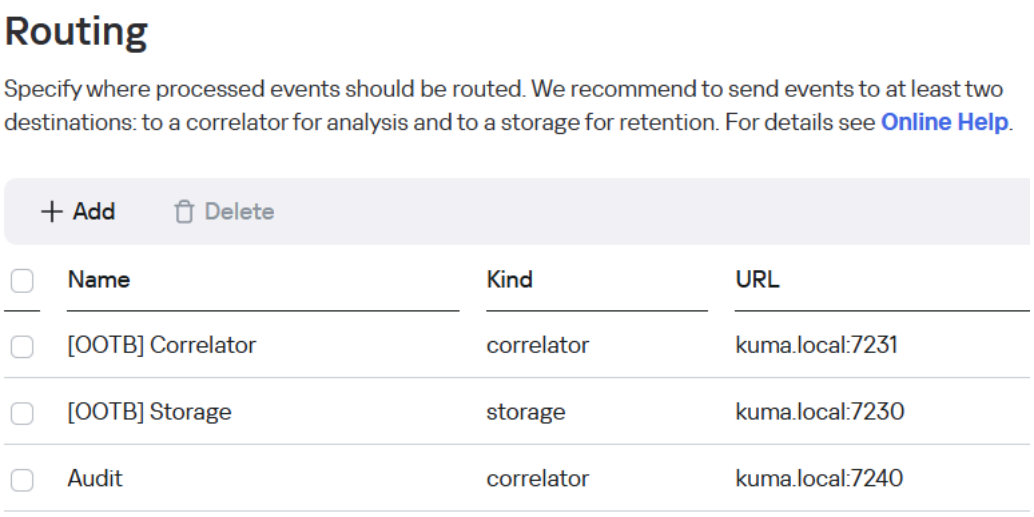
9. На вкладке **Routing** нажмите **+Add** и заполните поля:

- **Kind** – выберите `correlator`. После этого появится поле **URL**.
- **URL** – выберите доступный [OOTB] Correlator.

  Если необходима дополнительная обработка получаемых событий, то потребуется выполнить настройку коррелятора Audit. Создание нового коррелятора можно выполнить позже.
- **Name** – автоматически будет заполнено после выбора в поле **URL**.

10. На вкладке **Routing** нажмите **+Add** и заполните поля:

    - **Kind** – выберите `correlator`. После этого появится поле **URL**.
    - **URL** – выберите `Audit`.
    - **Name** – автоматически будет заполнено после выбора в поле **URL**.



Параметры коллектора на вкладке **Routing** в KUMA

11. На вкладке **Setup validation** нажмите **Create and save service** и получите команду запуска, которую необходимо выполнить через CLI на сервере KUMA.

12. Нажмите **Save**.

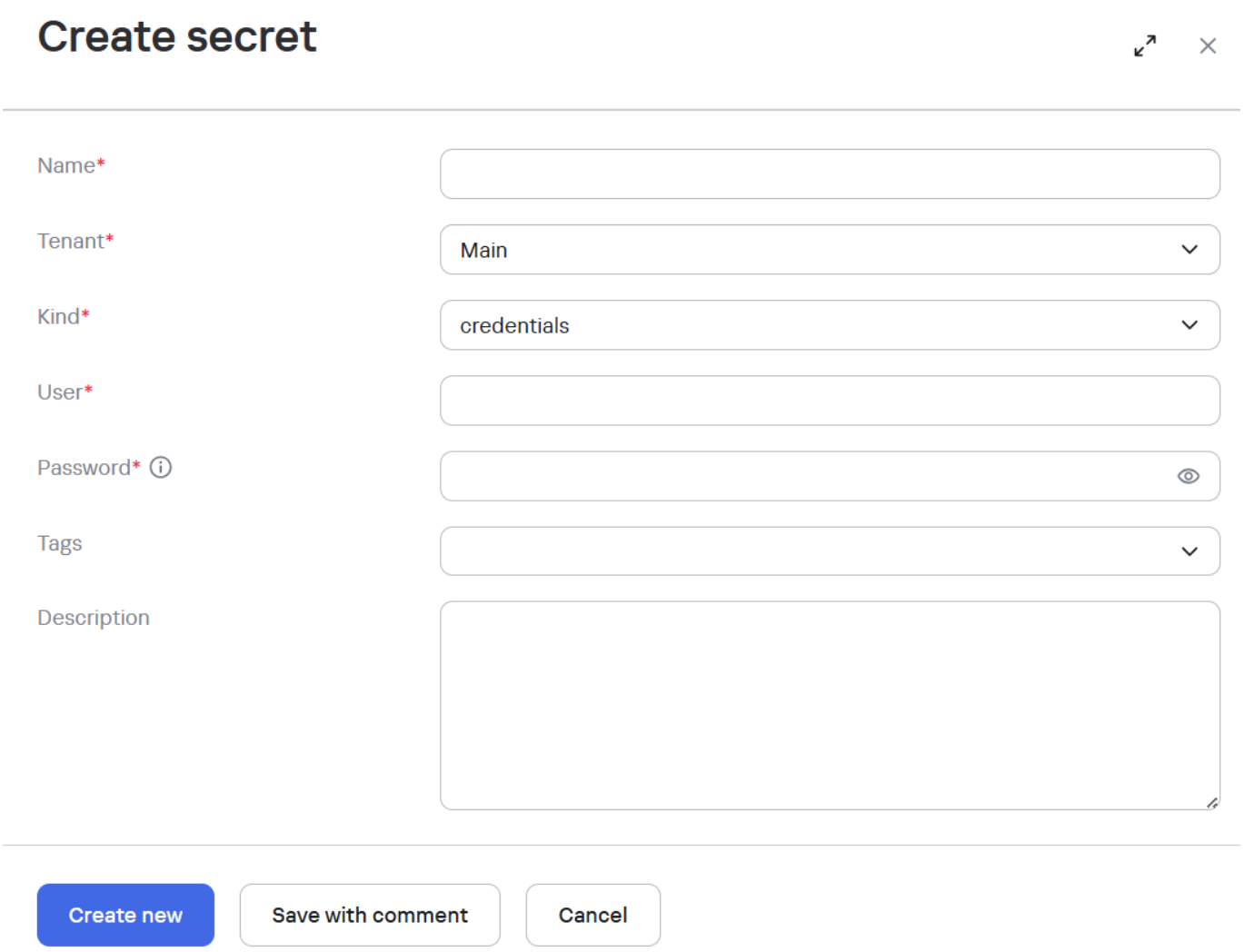
    Изменения будут сохранены.

Настройка почтовой службы в KUMA

Для получения уведомлений на почту от системных служб KUMA и событий, настроенных пользователем, необходимо выполнить настройку SMTP-сервера.

Чтобы настроить почтовую службу:

1. Перейдите в раздел **Resources** → **Secrets**.
2. Нажмите **+Create** и заполните поля:
   - **Name** – название политики.
   - **Tenant** – `Main` (выберите другой, если требуется).
   - **Kind** – `credentials`.
   - **User** – учетная запись на SMTP-сервере.
   - **Password** – пароль от учетной записи на SMTP-сервере.
   - **Tags** – не обязательно.
   - **Description** – не обязательно.

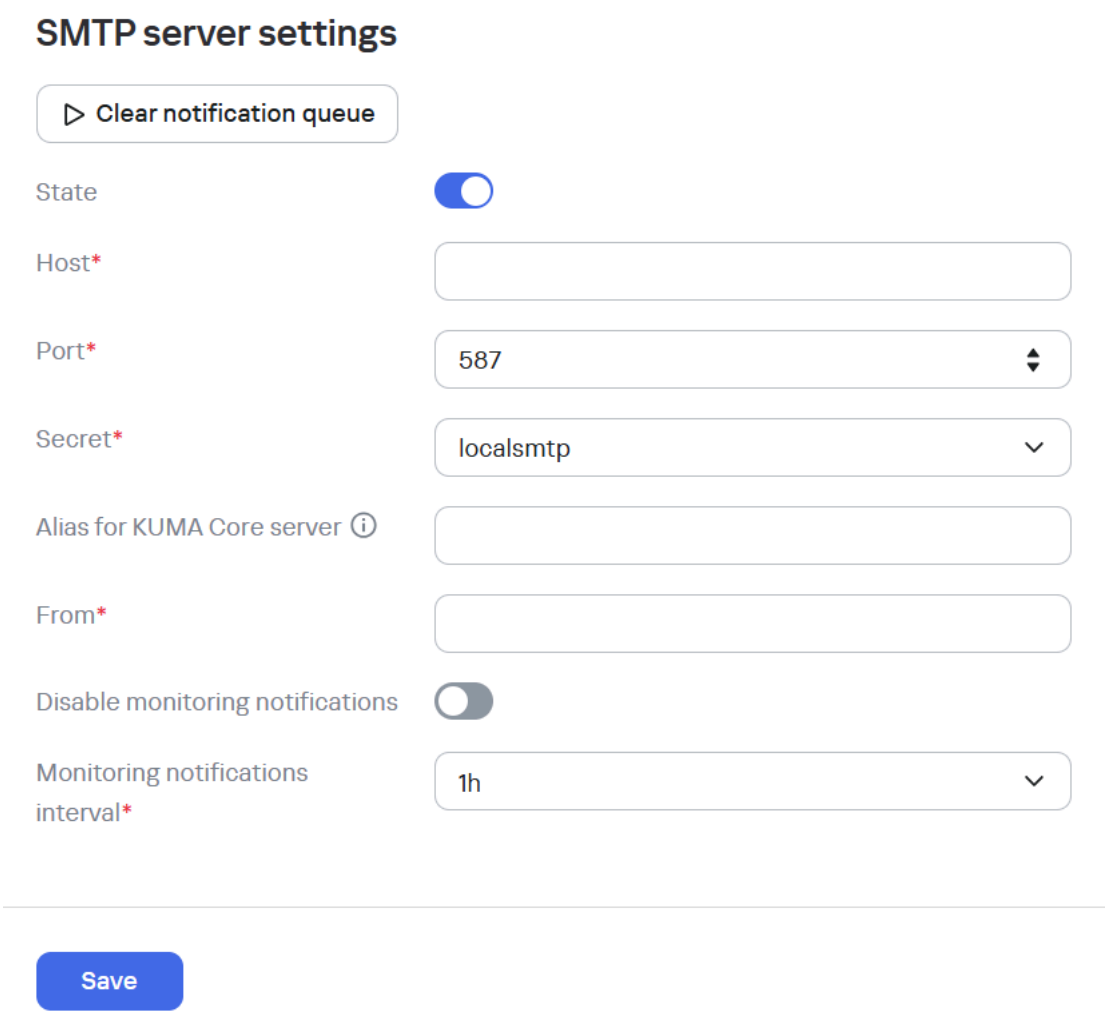


Параметры почтовой службы в разделе **Resources** → **Secrets** в KUMA

3. Перейдите в раздел **Settings** → **Other** → **Common**.

4. В разделе **SMTP server settings** заполните поля:

- **State** – переведите в положение "включено".
- **Host** – укажите IP-адрес или FQDN SMTP-сервера.
- **Port** – укажите порт службы SMTP-сервера.
- **Secret** – выберите политику, настроенную ранее.
- **Alias for KUMA Core server** – не обязательно.
- **From** – укажите почту, от имени которой будет производиться отправка писем пользователю.
- **Disable monitoring notifications** – оставьте без изменений.
- **Monitoring notifications interval** – `1h` (выберите другое значение, если требуется).

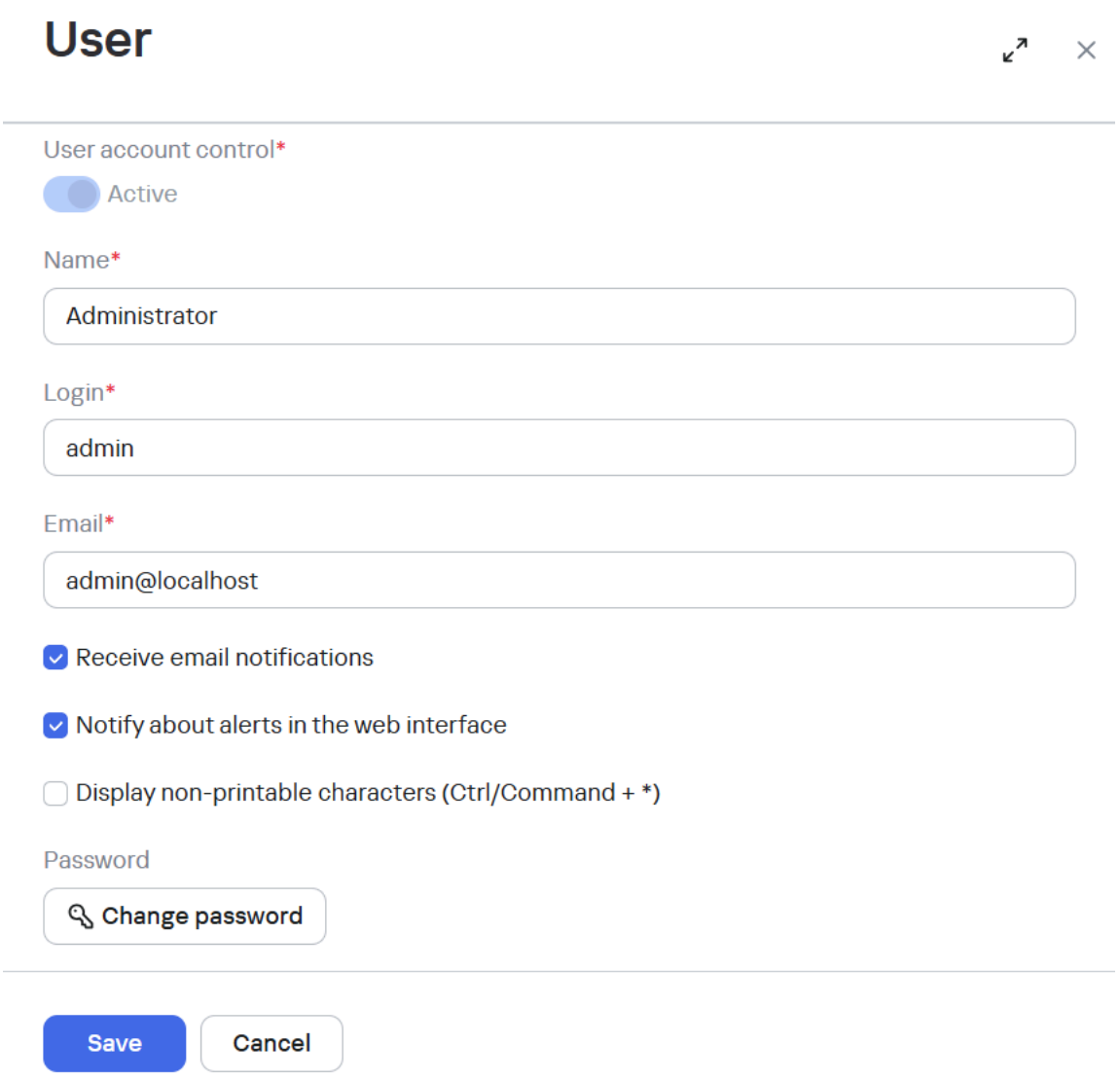


Параметры почтовой службы в разделе **Settings** → **Other** → **Common** в KUMA

5. Для активации отправки почтовых сообщений перейдите в профиль пользователя Administrator (**Administrator** → **Profile**) и заполните поля:

- **Email** – укажите почту пользователя Administrator.
- **Receive email notifications** – заполните флажок.

- **Notify about alerts in the web interface** – заполните флажок.



Профиль пользователя Administrator в KUMA

Изменения будут сохранены.

Настройка правил уведомления в KUMA

Для получения уведомлений на электронную почту пользователя об алертах от оркестратора SD-WAN и CPE необходимо выполнить настройку правил уведомления.

Чтобы настроить правила уведомления:

1. Перейдите в раздел **Settings** → **Other** → **Alerts** и выберите вкладку **Notification rules**.

2. Нажмите **+Add settings for a new tenant** и заполните поля.

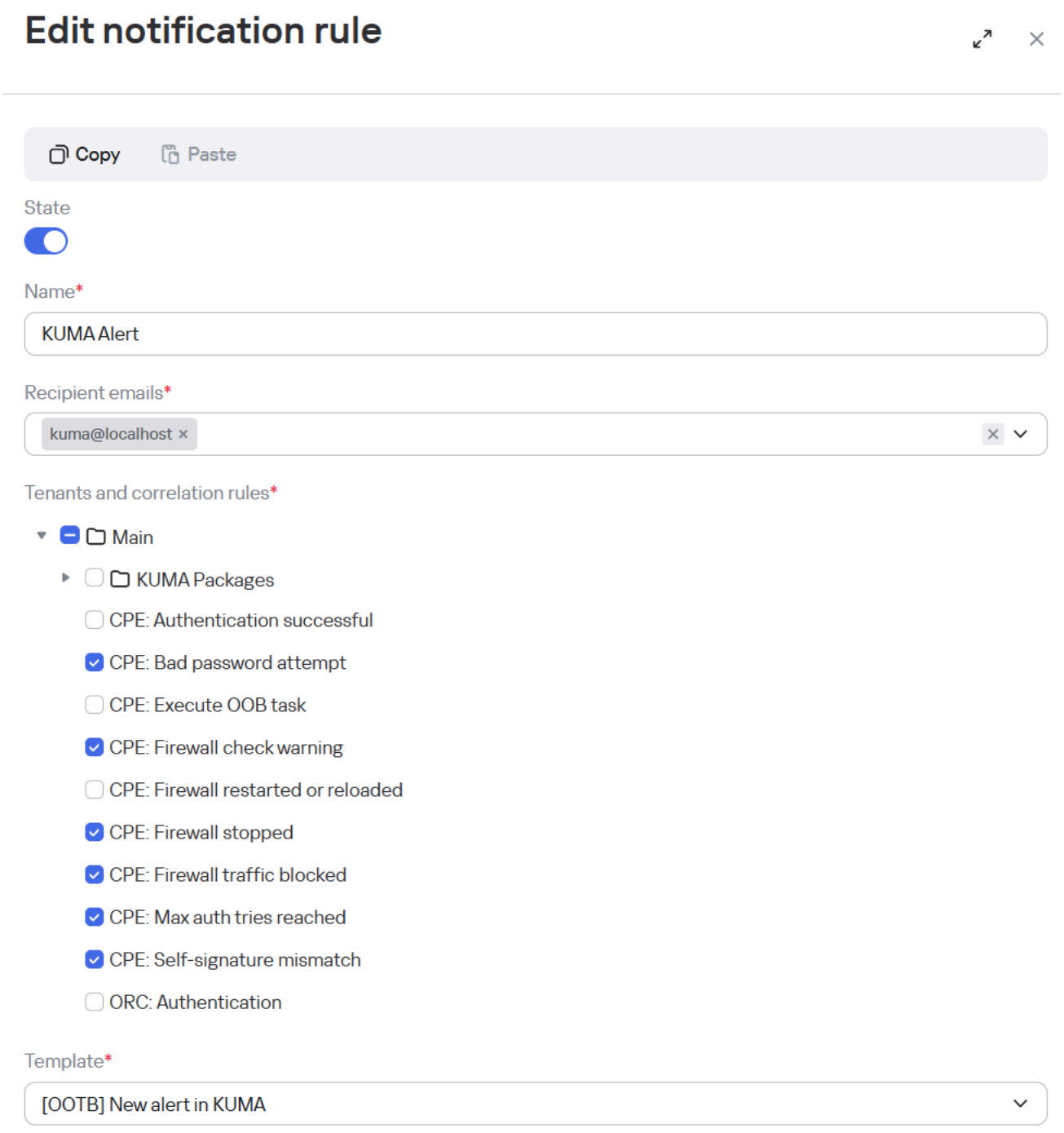
   - **State** – переведите в положение "включено".

   - **Tenant** – `Main` (выберите другой, если требуется).

3. Нажмите **+Add** и заполните поля:

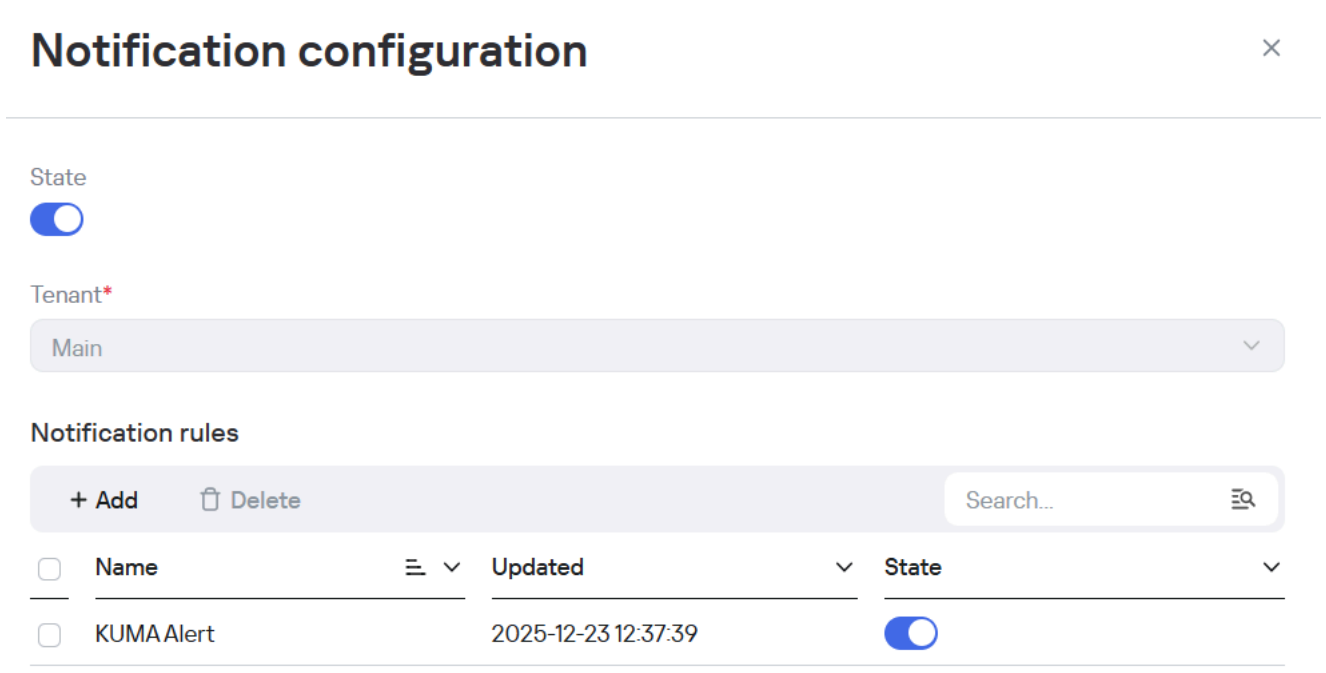
- **State** – переведите в положение "включено".
- **Name** – название правила (например, KUMA Alert).
- **Recipient emails** – почтовый(ые) адрес(а) пользователя(ей).
- **Tenants and correlation rules** – выберите правила, по которым хотите получать уведомления на почту.
- **Template** – выберите шаблон письма по умолчанию `[OOTB] New alert in KUMA` или создайте свой шаблон.

4. Нажмите **Save**.



Параметры правила уведомления в KUMA

5. Нажмите **Save**.



Параметры правил уведомления в KUMA

Изменения будут сохранены.

Примеры настройки для поиска по ключевым событиям в KUMA

Для поиска определенных событий безопасности можно воспользоваться SQL-вызовом напрямую в базу данных (в разделе **Events** → **SQL builder**). С помощью SQL Builder можно создать необходимые запросы и сохранить их для быстрых вызовов.

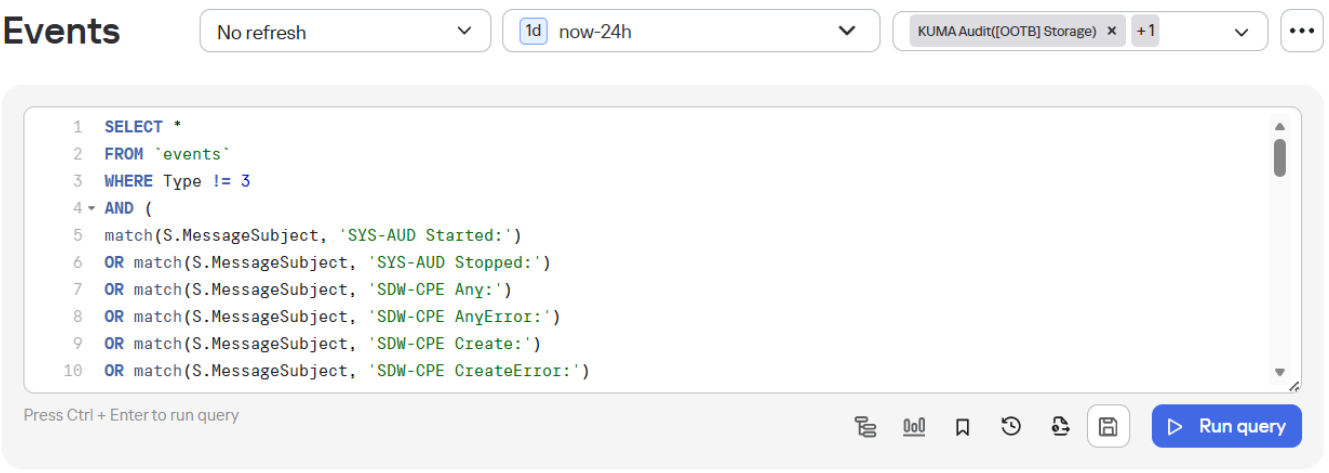
Выполнение SQL-запроса

Чтобы выполнить SQL-запрос:

1. Перейдите в раздел **Events** и найдите поле **Events** с SQL-запросом по умолчанию.

2. Удалите содержимое SQL-запроса по умолчанию.

3. Скопируйте и вставьте SQL-запрос из примеров этого раздела.

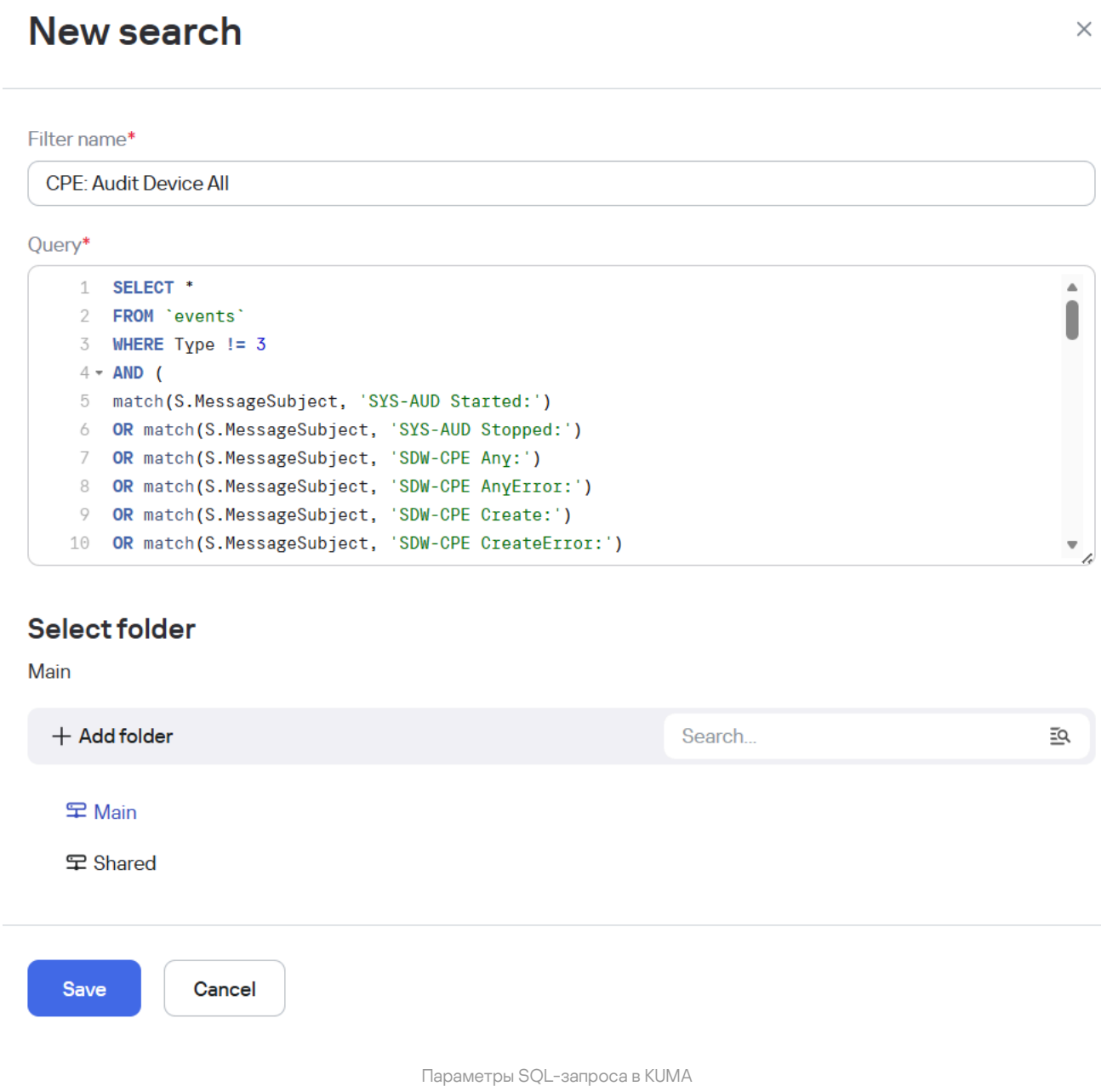


Раздел **Events** в KUMA

4. Нажмите **Save current filter** и заполните поля:

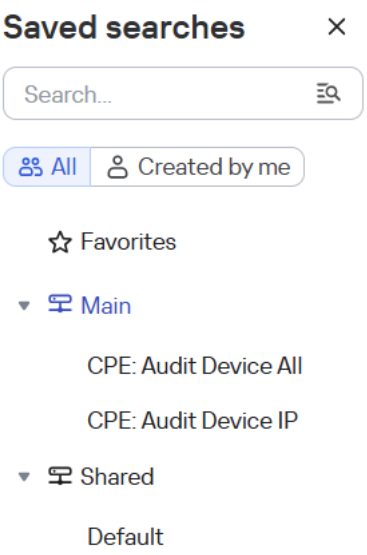
- **Filter name** – название SQL-запроса.
- **Query** – текст SQL-запроса.
- **Select folder** – выберите `Main`.

5. Нажмите **Save**, чтобы сохранить запрос.



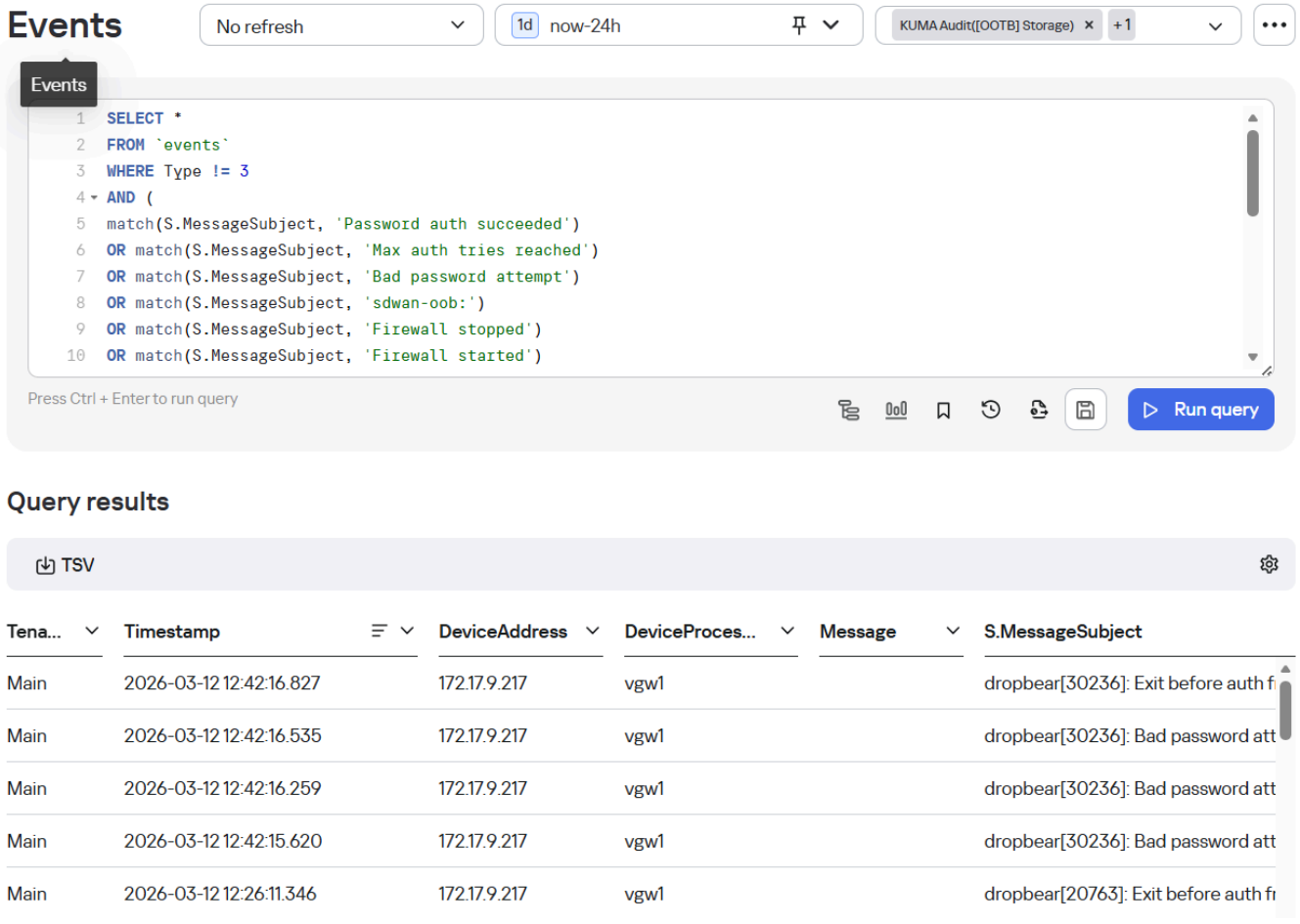
Параметры SQL-запроса в KUMA

6. Нажмите **Saved searches**, чтобы увидеть сохраненные SQL-запросы.



Сохраненные SQL-запросы в KUMA

7. Выберите необходимый SQL-запрос и нажмите **Run query** для отображения всех событий, соответствующих запросу.



Результат выполнения SQL-запроса в KUMA

Примеры SQL-запросов

Имя: ORC: Audit All Security notification

Описание: Для поиска всех событий безопасности на CPE (Исключаем правила корреляции, которые информируют о создании Alarm Type != 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;
```

Имя: CPE: Audit All Device

Описание: Для поиска всех событий безопасности на 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;
```

Имя: CPE: Audit All Device IP

Описание: Для поиска всех событий безопасности на CPE по определенному IP-адресу

```
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
LIMIT 500;
```

Интеграция с Kaspersky CyberSecurity for Networks

Вы можете интегрировать Kaspersky SD-WAN с программой Kaspersky Industrial CyberSecurity for Networks, чтобы передавать SPAN-трафик от сервисных интерфейсов устройств CPE на сетевые интерфейсы узлов Kaspersky Industrial CyberSecurity for Networks. Перед настройкой интеграции вам нужно включить шифрование трафика на устройствах CPE, от сервисных интерфейсов которых вы планируете передавать SPAN-трафик. Мы рекомендуем разместить устройства CPE в выделенной сети Kaspersky Industrial CyberSecurity.

Идентификация SPAN-трафика выполняется за счет добавления меток VLAN в пакеты трафика в соответствии со стандартом IEEE 802.1q. Вам нужно обеспечить соответствие меток VLAN, используемых на сервисных интерфейсах устройств CPE и на сетевых интерфейсах узлов Kaspersky Industrial CyberSecurity for Networks.

Для эффективной интеграции Kaspersky SD-WAN с Kaspersky Industrial CyberSecurity for Networks вы можете расширить ограничения на количество точек мониторинга путем дополнительной настройки компонентов Kaspersky Industrial CyberSecurity for Networks. Максимально возможные ограничения:

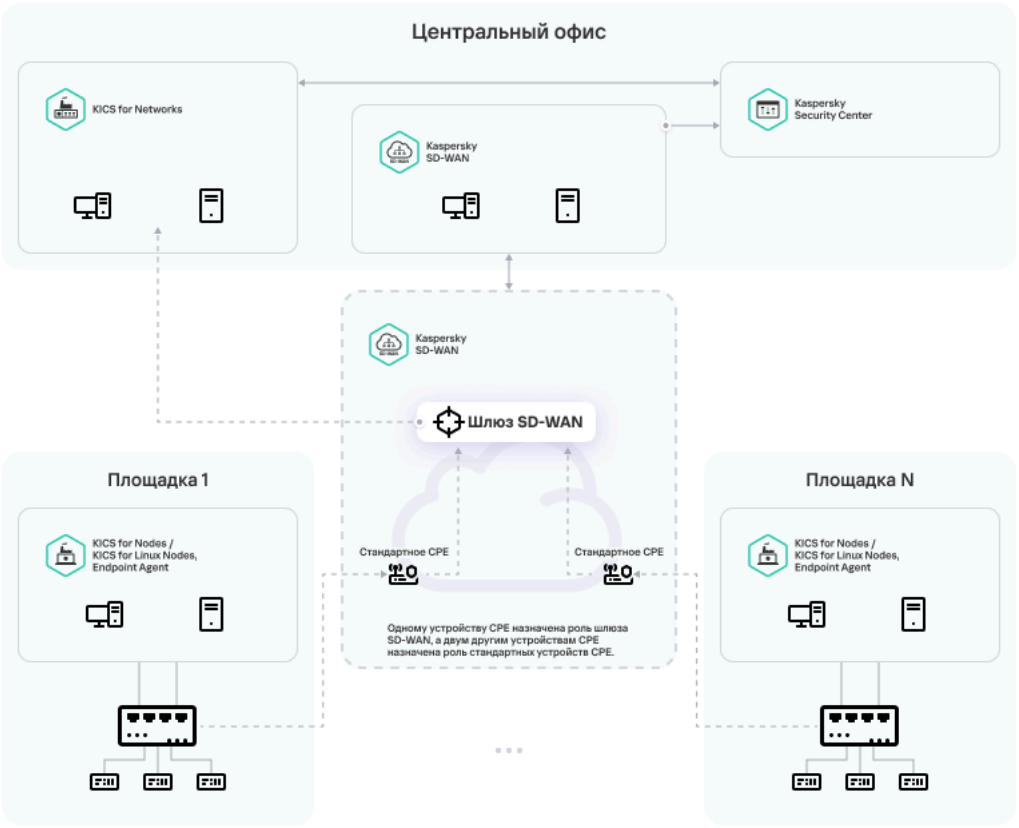
- не более 100 точек мониторинга на узле Kaspersky Industrial CyberSecurity for Networks;
- не более 100 точек мониторинга всего в Kaspersky Industrial CyberSecurity for Networks.

Остальные требования к развертыванию компонентов Kaspersky Industrial CyberSecurity for Networks аналогичны другим типовым схемам развертывания, например для схемы установки сервера без внешних сенсоров.

Для получения дополнительных сведений о настройке компонентов Kaspersky Industrial CyberSecurity for Networks при интеграции с Kaspersky SD-WAN вы можете обратиться к вашему персональному техническому менеджеру (TAM).

Вы можете получить дополнительную информацию об интеграции Kaspersky SD-WAN и Kaspersky Industrial CyberSecurity for Networks в разделе Приложения.

На рисунке ниже показан пример схемы развертывания Kaspersky SD-WAN и Kaspersky Industrial CyberSecurity for Networks. Пунктирными линиями обозначен путь передачи SPAN-трафика. Сначала сетевые коммутаторы на удаленных площадках 1 и N зеркалируют трафик на устройства CPE с ролью стандартных устройств CPE. Затем стандартные устройства CPE передают SPAN-трафик на устройство CPE с ролью шлюза SD-WAN, которое в свою очередь передает SPAN-трафик на сервер Kaspersky Industrial CyberSecurity for Networks. Компоненты Kaspersky SD-WAN и Kaspersky Industrial CyberSecurity for Networks находятся в центральном офисе организации.



Пример интеграции Kaspersky SD-WAN с Kaspersky Industrial CyberSecurity for Networks

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky SD-WAN, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky SD-WAN.

Kaspersky предоставляет поддержку Kaspersky SD-WAN в течение жизненного цикла (см. страницу жизненного цикла приложений). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих приложения "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;

- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Источники информации о решении

Этот раздел содержит описание источников информации о решении.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

Страница Kaspersky SD-WAN на веб-сайте "Лаборатории Касперского"

На странице Kaspersky SD-WAN вы можете получить общую информацию о решении, его возможностях и особенностях работы.

Страница Kaspersky SD-WAN содержит ссылку на интернет-магазин. В нем вы можете приобрести решение или продлить право пользования решением.

Страница Kaspersky SD-WAN в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky SD-WAN в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании решения.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky SD-WAN, но и к другим приложениям "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Обсуждение приложений "Лаборатории Касперского" на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Приложения

Вы можете получить дополнительную информацию о Kaspersky SD-WAN из следующих руководств:

- Руководство по развертыванию демонстрационного стенда Kaspersky SD-WAN в среде VMware, часть 1.
- Руководство по развертыванию демонстрационного стенда Kaspersky SD-WAN в среде VMware, часть 2.
- Руководство по эксплуатации KESR Model 1.
- Руководство по эксплуатации KESR Model 2 (исполнение 1).
- Руководство по эксплуатации KESR Model 2 (исполнение 2).
- Руководство по эксплуатации KESR Model 3.
- Руководство по эксплуатации KESR Model 4 (исполнение 1).
- Руководство по эксплуатации KESR Model 4 (исполнение 2).
- Руководство по эксплуатации KESR Model 5 (исполнение 1).
- Руководство по эксплуатации KESR Model 5 (исполнение 2).
- Передача SPAN-трафика через фабрику SD-WAN для тестирования сценариев KICS.

Глоссарий

Customer Premise Equipment (CPE)

Телекоммуникационное оборудование, включая виртуальные машины, находящееся на клиентской площадке. Используется для подключения клиентской площадки к сети SD-WAN, построения соединений и передачи трафика между клиентскими площадками. Трафик может передаваться в центр обработки данных для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Open vSwitch (OVS)

Тип программного коммутатора, на основе которого создана прошивка устройства CPE. Данная реализация использует обработку пакетов на уровне ядра и подходит для большинства устройств.

Physical Network Function (PNF)

Сетевые функции, реализуемые в виде специализированного оборудования или виртуальных сущностей, созданных с помощью сторонних сред виртуализации. Оркестратор не управляет жизненным циклом физических сетевых функций.

Port security

Функция, которая повышает уровень безопасности сети на уровне Ethernet-портов коммутаторов и предотвращает не авторизованный доступ к сети, ограничивая количество MAC-адресов, которые могут быть связаны с одним физическим портом. Если функция включена, только доверенные устройства с заранее определенными MAC-адресами могут подключиться к сети.

Software-Defined Networking (SDN)

Технология построения сетей передачи данных, в которых плоскость управления сетью отделена от плоскости передачи данных и реализована программно с использованием централизованного SDN-контроллера.

Software-Defined Wide Area Network (SD-WAN)

Подход к построению программно-определяемых сетей с использованием глобальной вычислительной сети. Сети SD-WAN предоставляют возможность соединения локальных сетей и пользователей, находящихся в географически разнесенных локациях.

Switch Operating System (SWOS)

Тип программного коммутатора, на основе которого сделана прошивка устройства CPE. Представляет собой альтернативную реализацию с обработкой пакетов на основе DPDK. Может демонстрировать увеличенную производительность благодаря обработке пакетов в обход ядра.

Universal CPE (uCPE)

Устройства CPE с дополнительной поддержкой развертывания виртуальных сетевых функций. Устройство uCPE должно иметь достаточно аппаратных ресурсов для того, чтобы не задействовать центр обработки данных или облако при предоставлении виртуальных сетевых функций.

Virtual Deployment Unit (VDU)

Виртуальная машина, которая является хостом VNF и объединяет виртуальные вычислительные ресурсы, такие как ЦПУ и память, необходимые для работы программного обеспечения VNF, а также содержит определенные имплементации сетевой функции, например алгоритмы маршрутизации или логику балансировки нагрузки.

Несколько VDU могут быть объединены в составе одной VNF для обеспечения масштабирования и/или высокой доступности. VDU можно распределить между отдельными физическими серверами, не теряя при этом возможности управлять ими как единой VNF. VDU взаимодействуют друг с другом и другими VNF, чтобы выполнять требуемые функции в рамках сетевого сервиса.

Virtual Infrastructure Manager (VIM)

Управляет вычислительными и сетевыми ресурсами, а также ресурсами хранения в рамках инфраструктуры NFV. Используется для связи сетевых функций с помощью виртуальных соединений, подсетей и портов.

Может быть развернут в центре обработки данных или на устройстве uCPE. Развертывание VIM в центре обработки данных, подразумевает централизованное управление жизненным циклом VNF, в то время как VIM, развернутый на устройстве uCPE, позволяет доставлять VNF на удаленные площадки и управлять этими VNF локально. Развернутый VIM требуется добавить в веб-интерфейс оркестратора.

В качестве VIM используется облачная платформа OpenStack.

Virtual Network Function (VNF)

Сетевые функции, реализуемые в виде виртуальных машин на обычных компьютерных платформах COTS (Commercial Off The Shelf). Жизненным циклом виртуальных сетевых функций управляет оркестратор. Для развертывания виртуальных сетевых функций требуется наличие облачной платформы OpenStack.

Virtual Network Function Manager (VNFM)

Управляет Управляет жизненным циклом виртуальных сетевых функций с помощью SSH, плейбуков Ansible, скриптов и атрибутов Cloud-init.

Контроллер

Централизованно управляет наложенной сетью:

- строит сетевую топологию;
- создает транспортные сервисы;
- управляет устройствами CPE по протоколу OpenFlow;
- распределяет трафик между соединениями;
- обеспечивает мониторинг соединений и автоматически переключает трафик на резервное соединение, если основное соединение выходит из строя.

Для развертывания контроллера вам нужно развернуть физическую сетевую функцию контроллера, которая содержится в архиве установки. Контроллер управляется оркестратором.

Оркестратор

Контролирует инфраструктуру решения, выполняет функции оркестратора NFV (NFVO), а также управляет сетевыми сервисами и распределенными менеджерами VNF (VNFM). Вы можете управлять оркестратором с помощью веб-интерфейса и REST API при использовании внешних северных (англ. northbound) систем.

Пакет PNF

Пакет в формате TAR или ZIP, который содержит данные, необходимые для развертывания и управления PNF.

Пакет VNF

Пакет в формате TAR или ZIP, который содержит данные, необходимые для развертывания и управления VNF.

Плоскость передачи данных

Часть сети, обрабатывающая и передающая трафик между разными площадками и устройствами. Плоскость передачи данных использует сетевые протоколы и алгоритмы для эффективной маршрутизации и доставки трафика по сети. Состоит из устройств CPE.

Плоскость управления сетью

Управляющая часть сети, контролирующая процесс передачи пакетов трафика через устройства CPE. Выполняет такие функции как обнаружение сети, расчет маршрутов, приоритизация трафика и применение политик безопасности. Плоскость управления позволяет централизованно управлять сетью, предоставляя полномасштабный обзор всех выполняемых операций. Состоит из оркестратора и контроллера.

Тенант

Логическая сущность, в рамках которой развертывается отдельный экземпляр SD-WAN. Тенанту назначаются компоненты решения, например компоненты сетевого сервиса, пользователи и устройства CPE, после чего администраторы тенанта могут управлять назначенными компонентами. Например, вы можете создать отдельного тенанта для клиента вашей организации.

Транспортная стратегия

Механизм инкапсуляции транспортных сервисов, включающий в себя алгоритм добавления стека меток заголовков пакетов трафика и тип этих меток. Kaspersky SD-WAN временно поддерживает одну транспортную стратегию **Generic VNI Swapping Transport**.

Шлюз SD-WAN

Устройство CPE, которому назначена роль шлюза SD-WAN. Шлюзы SD-WAN строят соединения со всеми устройствами в сети, включая другие шлюзы SD-WAN, таким образом обеспечивая связность между всеми устройствами CPE и контроллером. Вы можете установить несколько шлюзов SD-WAN для отказоустойчивости.

Экземпляр SD-WAN

Развернутое решение Kaspersky SD-WAN для одного из тенантов вашей организации. Является изолированной сущностью и имеет собственные сетевые сервисы, устройства CPE и параметры качества обслуживания.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory является товарным знаком группы компаний Microsoft.

Ansible, CentOS, Red Hat – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Atom, Celeron, Intel и Xeon являются товарными знаками Intel Corporation или ее дочерних компаний.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Firefox является товарным знаком Mozilla Foundation в США и других странах.

Google Chrome – товарный знак Google LLC.

IBM – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

Intel и Xeon являются товарными знаками Intel Corporation или ее дочерних компаний.

Kraftway – зарегистрированный товарный знак ЗАО "Крафтвэй корпорэйшн ПЛС".

Linux, LTS – товарные знаки Linus Torvalds, зарегистрированные в США и в других странах.

Microsoft Edge и Windows являются товарными знаками группы компаний Microsoft.

MIPS – товарный знак или зарегистрированный в США и других странах товарный знак MIPS Technologies.

OpenStack – зарегистрированный товарный знак OpenStack Foundation в США и других странах.

OpenStreetMap является товарным знаком OpenStreetMap Foundation. Настоящий продукт не является аффилированным или поддерживаемым со стороны OpenStreetMap Foundation.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Safari – товарный знак Apple Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

VMware – зарегистрированный товарный знак и/или товарный знак VMware, Inc. в США и других странах.

Zabbix – зарегистрированный товарный знак Zabbix SIA.