kaspersky

Kaspersky SD-WAN

Содержание

О Kaspersky SD-WAN

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

Технология SDN отделает плоскость управления сетью (англ. control plane) от плоскости передачи данных (англ. data plane) и позволяет управлять сетевой инфраструктурой с помощью оркестратора и 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 туннелей для передачи трафика с учетом требований приложений к пропускной способности и качеству обслуживания. Поддерживаются следующие каналы 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, устройства).

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.

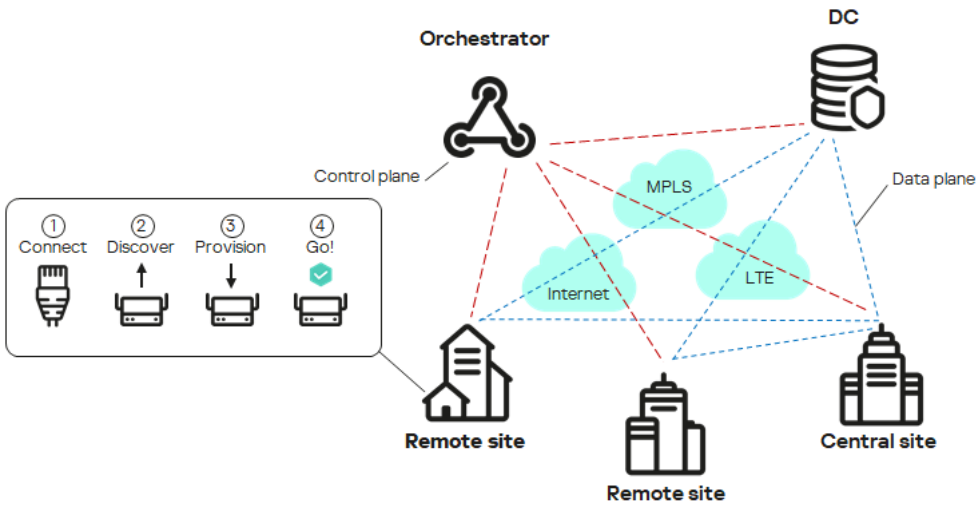


Схема сети SD-WAN

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:

- Мастер установки Kaspersky SD-WAN.
- 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:

Аппаратные требования

При развертывании решения вам нужно учитывать аппаратные требования для развертывания оркестратора, контроллера SD-WAN, VNFM, а также системы мониторинга. В Kaspersky SD-WAN используется система мониторинга Zabbix версии 5.0.26 и 6.0.0. Более подробную информацию об аппаратных требованиях к системе мониторинга можно получить из официальной документации решения Zabbix.

Требования к аппаратным ресурсам зависят от количества управляемых устройств CPE. Если требуется подключить более 250 устройств CPE, развертываются дополнительные кластеры контроллеров SD-WAN. При необходимости рассчитать более точные аппаратные требования для определенной схемы развертывания мы рекомендуем обратиться в техническую поддержку "Лаборатории Касперского".

- **Аппаратные требования при использовании до 50 устройств CPE**.

- Для развертывания оркестратора:
  - 8 ядер процессора;
  - 8 ГБ оперативной памяти;
  - 105 ГБ свободного дискового пространства;
  - 3 виртуальные машины.
- Для развертывания контроллера SD-WAN:
  - 4 ядра процессора;
  - 8 ГБ оперативной памяти;
  - 40 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания VNFM:
  - 4 ядра процессора;
  - 8 ГБ оперативной памяти;
  - 20 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания системы мониторинга:
  - 4 ядра процессора;
  - 8 ГБ оперативной памяти;
  - 100 ГБ свободного дискового пространства;
  - 3 контейнера.

- **Аппаратные требования при использовании до 100 устройств CPE**.

- Для развертывания оркестратора:
  - 8 ядер процессора;
  - 10 ГБ оперативной памяти;
  - 110 ГБ свободного дискового пространства;
  - 3 виртуальные машины.
- Для развертывания контроллера SD-WAN:
  - 6 ядер процессора;
  - 8 ГБ оперативной памяти;
  - 40 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания VNFM:
  - 4 ядра процессора;
  - 8 ГБ оперативной памяти;
  - 20 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания системы мониторинга:
  - 4 ядра процессора;
  - 10 ГБ оперативной памяти;
  - 200 ГБ свободного дискового пространства;
  - 3 контейнера.

- Аппаратные требования при использовании до 250 устройств CPE.

- Для развертывания оркестратора:
  - 8 ядер процессора;
  - 12 ГБ оперативной памяти;
  - 125 ГБ свободного дискового пространства;
  - 3 виртуальные машины.
- Для развертывания контроллера SD-WAN:
  - 8 ядер процессора;
  - 16 ГБ оперативной памяти;
  - 40 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания VNFM:
  - 4 ядра процессора;
  - 8 ГБ оперативной памяти;
  - 20 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания системы мониторинга:
  - 6 ядер процессора;
  - 12 ГБ оперативной памяти;
  - 350 ГБ свободного дискового пространства;
  - 3 контейнера.

- **Аппаратные требования при использовании до 500 устройств CPE**

- Для развертывания оркестратора:
  - 8 ядер процессора;
  - 16 ГБ оперативной памяти;
  - 150 ГБ свободного дискового пространства;
  - 3 виртуальные машины.
- Для развертывания контроллера SD-WAN:
  - 8 ядер процессора;
  - 16 ГБ оперативной памяти;
  - 40 ГБ свободного дискового пространства;
  - 6 контейнеров.
- Для развертывания VNFM:
  - 4 ядра процессора;
  - 8 ГБ оперативной памяти;
  - 20 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания системы мониторинга:
  - 8 ядер процессора;
  - 24 ГБ оперативной памяти;
  - 600 ГБ свободного дискового пространства;
  - 3 контейнера.

- **Аппаратные требования при использовании до 1000 устройств CPE.**

- Для развертывания оркестратора:
  - 10 ядер процессора;
  - 24 ГБ оперативной памяти;
  - 200 ГБ свободного дискового пространства;
  - 3 виртуальные машины.
- Для развертывания контроллера SD-WAN:
  - 8 ядер процессора;
  - 16 ГБ оперативной памяти;
  - 40 ГБ свободного дискового пространства;
  - 12 контейнеров.
- Для развертывания VNFM:
  - 4 ядра процессора;
  - 10ГБ оперативной памяти;
  - 20 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания системы мониторинга:
  - 10 ядер процессора;
  - 32 ГБ оперативной памяти;
  - 1100 ГБ свободного дискового пространства;
  - 3 контейнера.

- **Аппаратные требования при использовании до 5000 устройств CPE**.

- Для развертывания оркестратора:
  - 12 ядер процессора;
  - 32 ГБ оперативной памяти;
  - 600 ГБ свободного дискового пространства;
  - 3 виртуальные машины.
- Для развертывания контроллера SD-WAN:
  - 8 ядер процессора;
  - 16 ГБ оперативной памяти;
  - 40 ГБ свободного дискового пространства;
  - 60 контейнеров.
- Для развертывания VNFM:
  - 4 ядра процессора;
  - 12 ГБ оперативной памяти;
  - 20 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания системы мониторинга:
  - 12 ядер процессора;
  - 64 ГБ оперативной памяти;
  - 5100 ГБ свободного дискового пространства;
  - 3 контейнера.

- **Аппаратные требования при использовании до 10 000 устройств CPE**.

- Для развертывания оркестатора:
  - 16 ядер процессора;
  - 64 ГБ оперативной памяти;
  - 1100 ГБ свободного дискового пространства;
  - 5 виртуальных машин.
- Для развертывания контроллера SD-WAN:
  - 8 ядер процессора;
  - 16 ГБ оперативной памяти;
  - 40 ГБ свободного дискового пространства;
  - 120 контейнеров.
- Для развертывания VNFM:
  - 4 ядра процессора;
  - 16 ГБ оперативной памяти;
  - 20 ГБ свободного дискового пространства;
  - 3 контейнера.
- Для развертывания системы мониторинга:
  - 16 ядра процессора;
  - 128 ГБ оперативной памяти;
  - 10 100 ГБ свободного дискового пространства;
  - 3 контейнера.

Программные требования

Требуется платформа Docker версии 1.5 или выше. Поддерживаются следующие 64-разрядные операционные системы:

- Ubuntu версии 20 LTS и выше.
- Astra Linux версии 1.7 и выше (уровень защищенности: "Орел").

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.

В Kaspersky SD-WAN можно просмотреть топологию сети поверх карты. Для этого используются карты сервиса OpenStreetMap. 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 о картах вы можете получить из официальной документации сервиса OpenStreetMap.

Требования к устройствам CPE

Вы можете использовать стандартные устройства CPE и универсальные устройства CPE (англ. uCPE, далее устройства uCPE). В состав устройств uCPE входит гипервизор, поэтому на нем можно развернуть виртуальные сетевые функции и VIM.

Устройства CPE имеют прямой доступ в интернет (англ. Direct Internet Access, DIA) без перенаправления трафика в центральный офис.

Поддерживаются следующие устройства 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.

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

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 (Мбит/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
KESR-M5	IMIX (417)	2875
	Large (1300)	5750

Требования к общему хранилищу

Мы рекомендуем использовать собственное общее хранилище (англ. shared storage) для обеспечения отказоустойчивости. Существуют следующие требования к хранилищу:

- Поддержка одновременной записи и чтения с нескольких хостов.
- Размер зависит от размера размещаемых файлов, но не менее 40 ГБ доступного защищенного пространства, поддерживающего дальнейшее расширение.
- Пропускная способность канала передачи данных между хранилищем и оркестратором должна быть не менее 1 ГБит/с, рекомендуется использовать 10-гигабитный Ethernet или 8-гигабитный FC (Fiber Channel).
- Значение IOPS (input/output operations per second) должно быть не менее 250, рекомендуется не менее 400.
- Общее хранилище должно иметь один из следующих типов:
  - NFS.
  - iSCSI.
  - FC.
  - CephFS.
- Хранилище должно быть монтировано.
- Сохранение работоспособности при перезагрузке хоста.

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 своим компонентам (см. таблицу ниже).

Взаимодействующие компоненты	Протокол	Дополнительное обеспечение безопасности
Оркестратор и контроллер SD-WAN	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 SD-WAN и устройство CPE	OpenFlow 1.3.4	Для аутентификации и шифрования трафика между контроллером SD-WAN и устройством CPE используется протокол TLS.

Безопасное подключение устройств CPE

Решение использует следующие механизмы безопасного подключения устройств CPE:

- Обнаружение устройства CPE с помощью идентификатора DPID.
- Отложенная регистрация. Вы можете выбрать, в каком состоянии находится устройство CPE после успешной регистрации – *Активировано* или *Деактивировано*. Выключенное устройство CPE нужно включить, убедившись, что оно установлено на площадке.
- Двухфакторная аутентификация.

Использование виртуальных сетевых функций

Вы можете обеспечить дополнительный уровень безопасности с помощью виртуальных сетевых функций, разворачиваемых 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:

- Поддержано централизованное управление межсетевым экраном с использованием шаблонов и поддержкой функции DPI. Вы можете выключить или включить использование функции DPI при настройке основных параметров межсетевого экрана и указать марки DPI, чтобы применять правила межсетевого экрана к пакетам трафика приложений.
- Поддержано создание правил DNAT и SNAT при управлении межсетевым экраном для использования механизмов Source Network Address Translation (SNAT), Destination Network Address Translation (DNAT) и Port Address Translation (PAT). Вы можете централизованно управлять этими механизмами с помощью шаблонов межсетевого экрана.
- Поддержано использование до 200 виртуальных таблиц маршрутизации (VRF) на устройствах CPE. Вы можете помещать BGP-маршруты в одну из виртуальных таблиц маршрутизации.
- Поддержана установка цепочек сертификатов на устройствах CPE.
- Поддержано отслеживание информации о пакетах трафика с помощью протокола NetFlow версии 1, 5 и 9. Вы можете централизованно управлять протоколом с помощью шаблонов NetFlow.
- Информация о следующих событиях теперь отправляется на указанный вами Syslog-сервер:
  - вход и выход пользователя из веб-интерфейса оркестратора;
  - неправильный ввод пароля пользователем при входе в веб-интерфейс оркестратора;
  - блокировка пользователя, проводящего брутфорс-атаку;
  - попытка входа в веб-интерфейс оркестратора с использованием несуществующей учетной записи.
- Поддержана двухфакторная аутентификация пользователей с использованием алгоритма Time-based-one-time password (TOTP).
- Поддержка обновления Kaspersky SD-WAN с версии 2.1.3 до 2.2.0. Если вы используете версию ниже 2.1.3, вам нужно сначала обновить решение до 2.1.3, после чего до 2.2.0. Сначала необходимо обновить центральные компоненты решения, затем – устройства CPE.
- Добавлен мастер установки для быстрого развертывания Kaspersky SD-WAN. При использовании мастера установки вы можете изменять элементы веб-интерфейса оркестратора, например отображающийся логотип организации.
- Поддержана отправка уведомлений о событиях и проблемах на устройствах CPE на электронную почту пользователей.

- Поддержана диагностика устройства CPE с помощью следующих утилит:
  - ping;
  - traceroute;
  - tcpdump;
  - iperf;
  - sweep.
- Поддержана версия 6.0.0 системы мониторинга Zabbix.
- Поддержан шаблон OVF для виртуальных устройств CPE. Вы можете использовать этот шаблон, чтобы проводить автоматическую регистрацию устройства CPE с использованием гипервизора VMware ESXi.
- Оптимизация производительности контроллера SD-WAN и устройств CPE.
- Оптимизация восстановления вышедшего из строя узла контроллера SD-WAN.
- Поддержано создание диапазонов IP-адресов и подсетей для устройств CPE (IPAM). Вы можете использовать эти диапазоны для централизованного назначения IPv4-адресов сетевым интерфейсам устройств CPE. Диапазоны IP-адресов можно также использовать для централизованного назначения IPv4-адресов идентификаторам маршрутизатора (англ. router ID) устройств CPE.
- Имена устройств CPE теперь отображаются в системе мониторинга Zabbix.
- Поддержано помещение хостов устройств CPE, VNF и PNF в автоматически созданные группы на сервере Zabbix. Группы соответствуют тенантам, которым назначены VNF, PNF и устройства CPE.
- Поддержана операционная система РЕД ОС® 8 для центральных компонентов решения.
- Поддержано изменение пароля пользователями с ролью тенанта.
- Поддержано отображение назначенных IPv4-адресов в таблице сетевых интерфейсов устройства CPE.
- Поддержано создание сетевых интерфейсов для подключения к PPPoE-серверу.
- Поддержана передача multicast-трафика устройствами CPE с помощью протоколов PIM и IGMP.

Архитектура решения

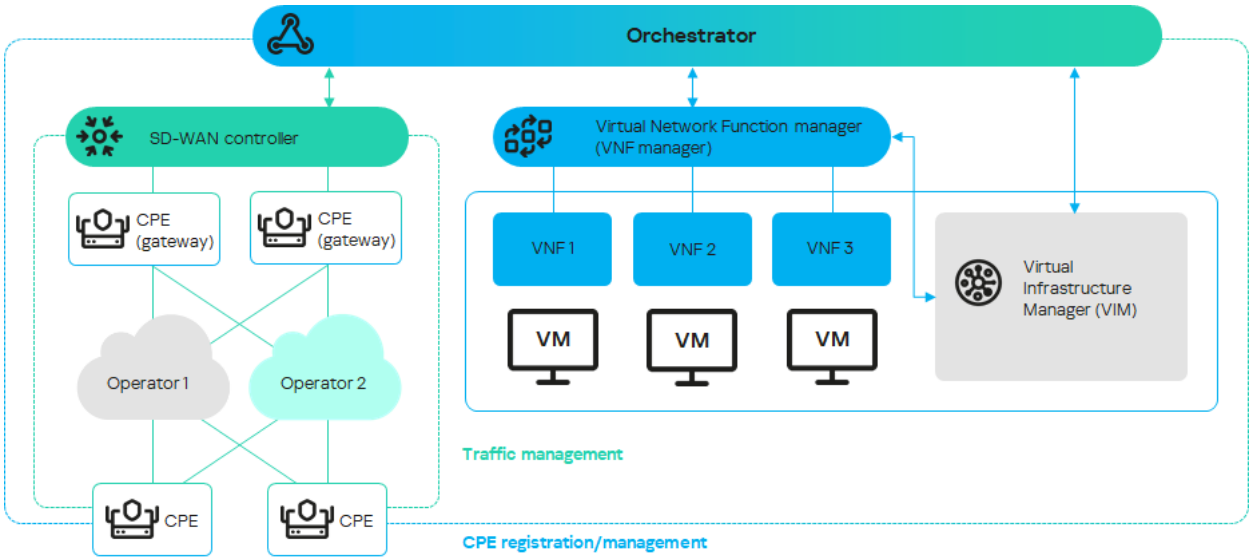
Kaspersky SD-WAN содержит следующие основные компоненты:

- Оркестратор – контролирует инфраструктуру решения, выполняет функции оркестратора NFV (NFVO), а также управляет сетевыми сервисами и распределенными VNFM. Может управляться с помощью веб-интерфейса и REST API при использовании внешних северных (англ. northbound) систем.
- Контроллер SD-WAN – централизованно управляет наложенной сетью и сетевыми устройствами в соответствии с топологией сервисной цепочки по протоколу OpenFlow. Развертывается как виртуальная или физическая сетевая функция.
- Устройства CPE – передают трафик и образуют SDN-фабрику в виде наложенной сети. Устанавливаются на удаленных площадках.
- VNFM – управляет жизненным циклом виртуальных сетевых функций с помощью SSH, сценариев Ansible, скриптов и атрибутов Cloud-init.

При использовании виртуальных сетевых функций в архитектуру могут входить следующие дополнительные компоненты:

- Контроллер SDN – управляет аппаратными и программными коммутаторами. Необязательный компонент.
- VIM – управляет вычислительными и сетевыми ресурсами, а также ресурсами хранения в рамках инфраструктуры NFV. Связывает VNF с помощью виртуальных каналов, подсетей и портов. Как VIM используется облачная платформа OpenStack.

Kaspersky SD-WAN имеет распределенную микросервисную архитектуру на основе Docker-контейнеров (см. рисунок ниже). Контроллер SD-WAN может состоять из одного, трех или пяти узлов. Узлы контроллера являются отдельными виртуальными машинами, которые можно запустить на разных аппаратных серверах, чтобы обеспечить отказоустойчивость.



Архитектура Kaspersky SD-WAN

Установка Kaspersky SD-WAN

Мастер установки KNAAS installer позволяет развернуть Kaspersky SD-WAN в соответствии с требуемой схемой развертывания. В комплект поставки входит архив в формате TAR.GZ с именем <knaas-installer_<версия>. Этот архив имеет следующую структуру

- Файл ansible.cfg – системный файл с параметрами Ansible.
- Файл CHANGELOG.md – журнал изменений файлов в формате YAML в составе мастера установки.
- Директория docs – документация по использованию мастера установки.
- Директория images – образы развертываемых компонентов решения.
- Директория inventory:
  - Директория external:
    - Директория pnf – примеры файлов для типовых схем развертывания решения с контроллером SD-WAN в виде физических сетевых функций.
    - Директория vnf – примеры файлов для типовых схем развертывания решения с контроллером SD-WAN в виде виртуальных сетевых функций.
  - Директория generic – общие системные файлы.
- Директория knaas – системные файлы с плейбуками, которые вызываются при развертывании решения.
- Директория oem – элементы веб-интерфейса оркестратора, которые можно изменить. Например, с помощью этой директории вы можете изменить логотип организации.
- Директория pnfs – примеры физических сетевых функций для развертывания контроллера SD-WAN.
- Файл README.md – инструкция по развертыванию решения с помощью мастера установки.
- Файл requirements.txt – системный файл с требованиями для Python.

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

Если у вас возникают проблемы с развертыванием Kaspersky SD-WAN с помощью мастера установки, мы рекомендуем обратиться в техническую поддержку "Лаборатории Касперского".

Резервирование центральных компонентов решения

Kaspersky SD-WAN поддерживает две схемы развертывания компонентов: N+1 и 2N+1.

В *схеме развертывания N+1* вместе с активным компонентом вам нужно развернуть резервный компонент. Если активный компонент выходит из строя, резервный компонент занимает его место.

В *схеме развертывания 2N+1* вам нужно дважды развернуть активный компонент и вместе с ним развернуть резервный компонент. Компоненты синхронизированы между собой, и один может занять место другого, если возникает неполадка. Такая схема резервирования позволяет компонентам сохранять работоспособность, даже когда происходит несколько аварий подряд.

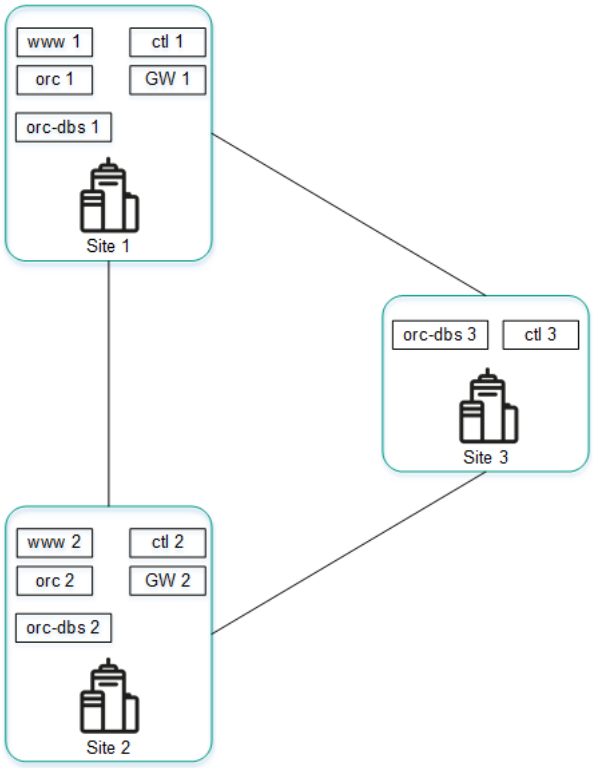
В таблице ниже представлены схемы резервирования и протоколы, которые используются для разных компонентов решения.

Компонент	Схема резервирования	Используемый протокол
Оркестратор	N+1	REST
Веб-интерфейс оркестратора	N+1	REST
База данных оркестратора	2N+1	MONGODB
Контроллер SD-WAN и его база данных	2N+1	OPENFLOW (TLS)
Шлюз SD-WAN	N+1	GENEVE

Пример размещения компонентов решения на географически разнесенных площадках представлен на рисунке ниже. На всех последующих рисунках используются следующие условные обозначения:

- оркестратор – orc;
- веб-интерфейс оркестратора – www;
- база данных оркестратора – orc-dbs;
- контроллер SD-WAN и его база данных – ctl;
- шлюз SD-WAN – GW.

Для компонентов решения, которые резервируются по схеме N+1, развертываются два узла на разных площадках. Каждый из узлов находится в активном состоянии. Вы можете выбрать узел, к которому направляются запросы, с помощью виртуального IP-адреса или службы DNS.

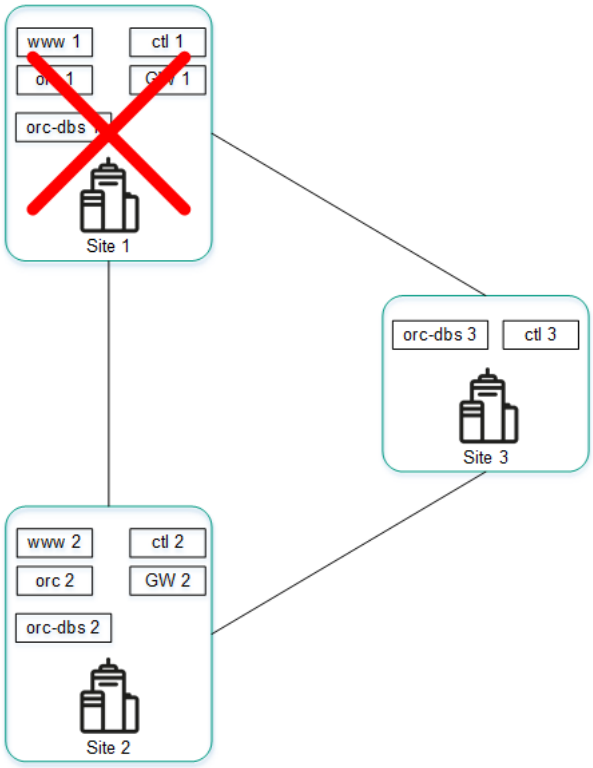


Размещение компонентов решения на географически разнесенных площадках

Компоненты, которые резервируются по схеме 2N+1, образуют кластер. Этот кластер содержит один основной узел и два резервных. Вы можете назначить один из узлов арбитром для экономии ресурсов и снижения требований к туннелям.

Если узел кластера назначен арбитром, он не содержит базу данных, и вы не можете сделать его основным. Узел-арбитр участвует в голосовании при выборе основного узла и обменивается с другими узлами периодическими контрольными пакетами.

На рисунке ниже представлен пример аварии на одной из площадок и ответная реакция решения. В этом примере показана авария, в ходе которой выходят из строя узлы кластера компонентов решения на площадке 1.



Авария на площадке 1

Если узлы кластера компонентов решения на площадке 1 выходят из строя, происходят следующие события:

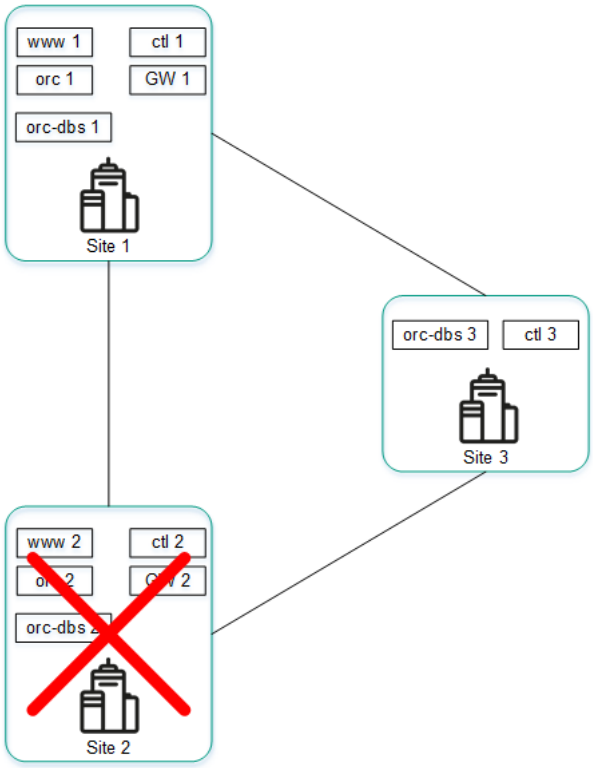
1. Узел orc-dbs 2 и узел-арбитр orc-dbs 3 теряют связь с узлом orc-dbs 1, после чего выбирают новый основной узел.

2. Узел-арбитр orc-dbs 3 не может быть основным узлом, поэтому им становится узел orc-dbs 2 и сообщает оркестратору о своей роли.

3. Узел ctl 2 и узел-арбитр ctl 3 теряют связь с узлом ctl 1, после чего выбирают новый основной узел.

4. Узел-арбитр ctl 3 не может быть основным узлом, поэтому им становится узел ctl 2 и сообщает оркестратору о своей роли.

На рисунке ниже представлен пример аварии, в ходе которой выходят из строя узлы кластера компонентов решения на площадке 2.



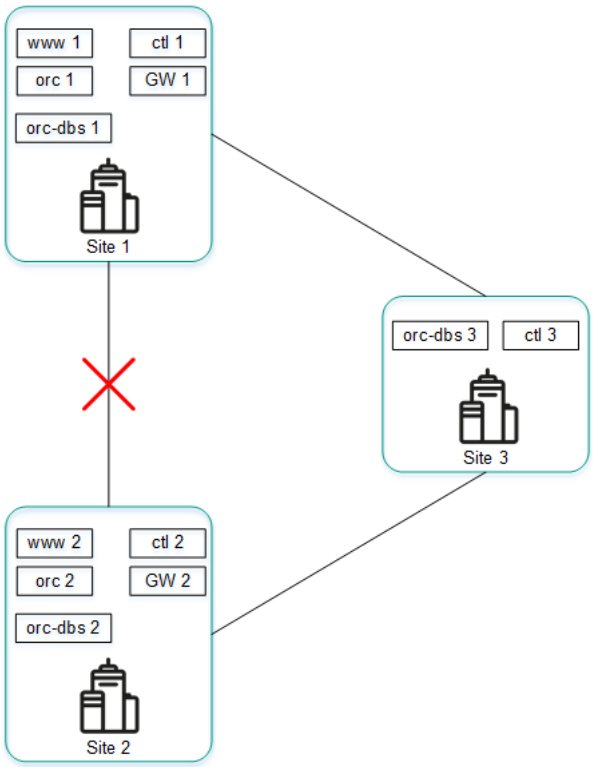
Авария на площадке 2

Если узлы кластера компонентов решения на площадке 2 выходят из строя, происходят следующие события:

1. Узел orc-dbs 1 и узел-арбитр orc-dbs 3 теряют связь с узлом orc-dbs-2, после чего узел orc-dbs 1 остается основным узлом.

2. Узел ctl 1 и узел-арбитр ctl 3 теряют связь с узлом ctl 2, после чего узел ctl 1 остается основным узлом.

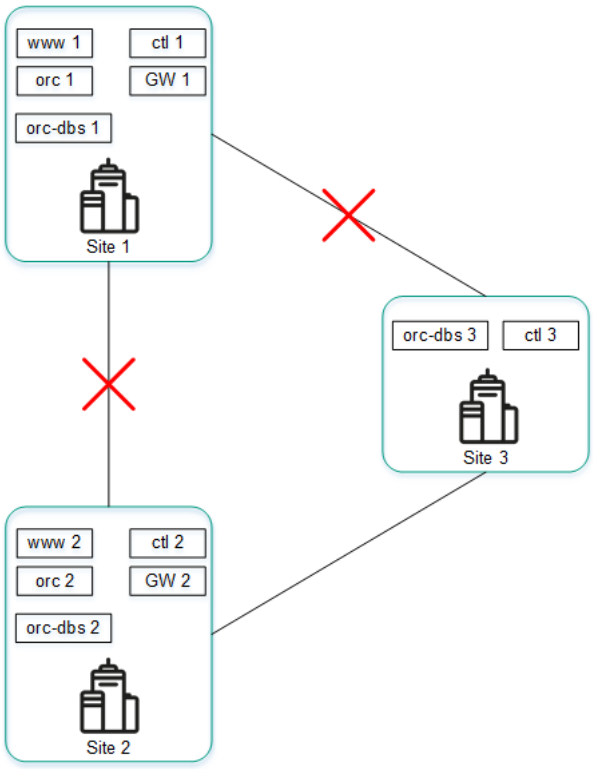
На рисунке ниже представлен пример аварии, в ходе которой прерывается соединение между площадками 1 и 2.



Если узлы кластера компонентов решения на площадках 1 и 2 не могут установить соединение друг с другом, происходят следующие события:

1. Узел orc-dbs 1 теряет связь с узлом orc-dbs 2.
2. Узел orc-dbs 1 остается основным узлом, потому что узел-арбитр orc-dbs 3 видит, что обе площадки работают в штатном режиме.
3. Узел ctl 1 теряет связь с узлом ctl 2.
4. Узел ctl 1 остается основным узлом, потому что узел-арбитр ctl 3 видит, что обе площадки работают в штатном режиме.

На рисунке ниже представлен пример аварии, в ходе которой прерывается соединение между площадкой 1 и остальными площадками.



Авария на соединениях между площадкой 1 и остальными площадками

Если узлы кластера компонентов решения на площадке 1 не могут установить соединение с остальными площадками, происходят следующие события:

1. Узел orc-dbs 1 теряет связь с узлом orc-dbs 2.
2. Узел orc-dbs 2 становится основным узлом и сообщает оркестратору о своей роли, потому что узел-арбитр orc-dbs 3 видит, что площадка 1 недоступна.
3. Узел ctl 1 теряет связь с узлом ctl 2.
4. Узел ctl 2 становится основным узлом и сообщает оркестратору о своей роли, потому что узел-арбитр ctl 3 видит, что площадка 1 недоступна.

Вход и выход из веб-интерфейса оркестратора

Вход в веб-интерфейс оркестратора

Чтобы войти в веб-интерфейс оркестратора:

1. В адресной строке браузера введите IP-адрес или имя сервера Kaspersky SD-WAN.
2. На открывшейся странице аутентификации введите имя пользователя и пароль. Пароль должен содержать как минимум один прописной и строчный символ A–Z, цифру и 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 кнопку 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 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

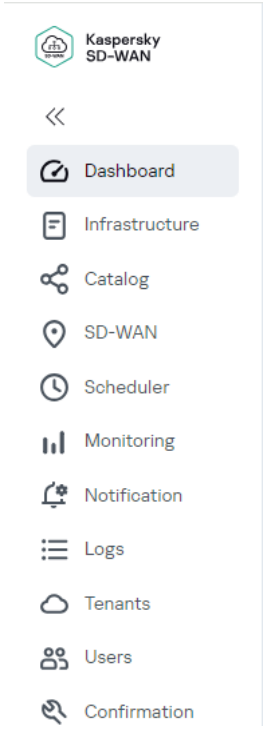
Управление Kaspersky SD-WAN осуществляется с помощью веб-интерфейса оркестратора. Отображающиеся в меню разделы можно использовать для настройки компонентов решения. Когда вы переходите в раздел, отображается дополнительное меню с подразделами в свернутом виде. Вам нужно навести курсор мыши на значок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

Поддерживается две версии 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 в портал самообслуживания тенанта.

Портал администратора

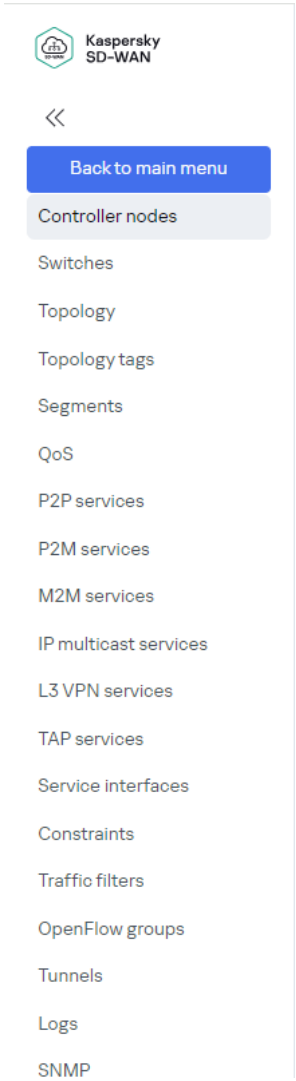


Основное меню портала администратора

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

Каталог	Шаблоны для централизованной настройки сетевых сервисов.
SD-WAN	• **Устройства CPE** – устройства CPE для передачи трафика. • **Шаблоны CPE** – шаблоны CPE для централизованной настройки устройств. • **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. • **Прошивка** – прошивки устройств CPE. • **Сертификаты** – сертификаты для установки на устройствах CPE. • **Экземпляры SD-WAN** – развернутые экземпляры SD-WAN. • **Шаблоны экземпляров SD-WAN** – шаблоны экземпляра SD-WAN для централизованной настройки и развертывания экземпляров. • **Пулы экземпляров SD-WAN** – пулы экземпляров SD-WAN. • **Шаблоны UNI** – шаблоны UNI для централизованного создания UNI на устройствах CPE.
Планировщик	Запланированные задачи.
Мониторинг	Параметры Zabbix-сервера для мониторинга компонентов решения.
Оповещения	Параметры отправки уведомлений пользователям на электронную почту.
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.

Определенные компоненты решения можно настроить в дополнительном меню настройки контроллера.

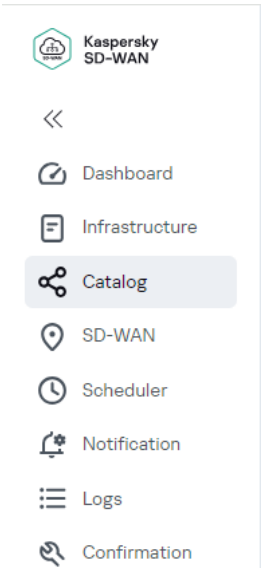


Меню настройки контроллера в портале администратора

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 топологии, например Hub-and-Spoke.
Сегменты	Сегменты, образованные из устройств CPE и коммутаторов.
QoS	Параметры качества обслуживания. В этом разделе вы можете настроить следующие компоненты: • классы трафика; • классификаторы трафика; • QoS-правила.
P2P-сервисы	Транспортные сервисы Point-to-Point.
P2M-сервисы	Транспортные сервисы Point-to-Multipoint.
M2M-сервисы	Транспортные сервисы Multipoint-to-Multipoint.
IP multicast-	Транспортные сервисы IP multicast.

сервисы	
L3 VPN-сервисы	Транспортные сервисы L3 VPN.
TAP-сервисы	Сервисы Test Access Point для зеркалирования трафика.
Сервисные интерфейсы	Сервисные интерфейсы устройств CPE и коммутаторов.
Ограничения	Пороговые ограничения для обеспечения качества обслуживания.
Фильтры трафика	Фильтры трафика для обеспечения качества обслуживания.
OpenFlow-группы	Группы OpenFlow-портов.
Туннели	Каналы между устройствами CPE и коммутаторами, а также туннели между устройствами CPE.
Журналы	Уровень детализации журналов Docker-контейнеров.
SNMP	Параметры мониторинга устройств CPE, а также виртуальных и физических сетевых функций с помощью протокола SNMP.

Портал самообслуживания

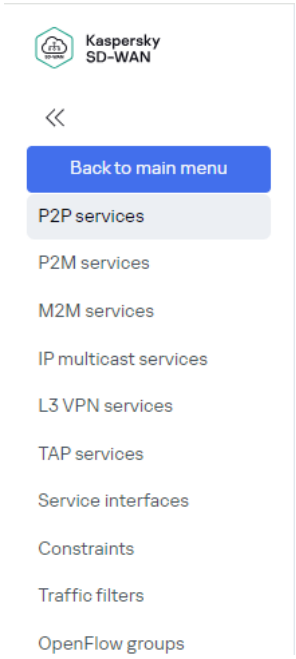


Основное меню портала самообслуживания

Обозреватель	Информация о текущем состоянии компонентов решения, таких как устройства CPE и сетевые функции.
Инфраструктура	Ресурсы организации. В этом разделе вы можете настроить контроллеры.
Каталог	Сетевые сервисы для передачи трафика и виртуализации сетевых функций.
SD-WAN	• **Устройства CPE** – устройства CPE для передачи трафика. • **Шаблоны CPE** – шаблоны CPE для централизованной настройки устройств. • **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	Запланированные задачи.
Оповещения	Параметры отправки уведомлений пользователям на электронную почту.
Журналы	Журналы компонентов решения, таких как устройства CPE, а также виртуальные и физические сетевые функции.
Подтверждение	Запросы на подтверждение действий пользователей.

Определенные компоненты решения можно настроить в дополнительном меню контроллера.



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	Сервисы Test Access Point для зеркалирования трафика.
Сервисные интерфейсы	Сервисные интерфейсы устройств CPE и коммутаторов.
Ограничения	Пороговые ограничения для обеспечения качества обслуживания.
Фильтры трафика	Фильтры трафика для обеспечения качества обслуживания.
OpenFlow-группы	Группы OpenFlow-портов.

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. В меню перейдите в раздел или подраздел веб-интерфейса оркестратора, который вы хотите установить как страницу по умолчанию.
2. В нижней части меню нажмите на значок настройки → **Сделать страницей по умолчанию**.

   В верхней части страницы отобразится сообщение `Страница по умолчанию установлена`.
3. Если вы хотите сбросить страницу по умолчанию, нажмите на значок настройки → **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,

в нижней части меню нажмите на значок настройки → **Темная тема** или **Светлая тема**.

Изменение языка веб-интерфейса оркестратора

Веб-интерфейс оркестратора поддерживает английский и русский язык.

Чтобы изменить язык веб-интерфейса оркестратора,

в нижней части меню нажмите на одну из следующих кнопок:

- **EN** – изменить язык веб-интерфейса оркестратора на английский.
- **RU** – изменить язык веб-интерфейса оркестратора на русский.

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 отображения записей с выбранным статусом.

- Фильтры времени для отображения 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.

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,

в нижней части меню нажмите на кнопку перехода к API .

Откроется список API-команд, доступных для управления оркестратором.

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 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 отдельных локальных пользователей, LDAP-пользователей и LDAP-групп.

Если двухфакторная аутентификация включена для пользователя, при следующем входе этого 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 пользователь должен 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, подразделы и действия доступны пользователям, и назначать эти права доступа при создании и изменении пользователя или группы 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 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, а отклоненные запросы 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. Время бездействия до автоматического выхода можно указать вручную.
- 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

Список прав доступа отображается 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 будет 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: 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**. По умолчанию флажок снят.

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 будет 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 в поле **Имя** введите имя права доступа. Максимальная длина: 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**. По умолчанию флажок снят.

6. 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 будет 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**.

Копия права доступа с новым именем будет создана 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 будет 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

Таблица LDAP-подключений отображается в разделе **Пользователи** на вкладке **LDAP-подключение**. 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 инструкции 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 будет выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **LDAP-подключение**.

   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 **Альтернативное имя 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 должен использовать 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 должен использовать для поиска учетных записей пользователей в директории удаленного сервера:

   - **uid (OpenLDAP)** – идентификатор пользователя UID (user ID) для поиска в OpenLDAP. Значение 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 котором 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 просмотреть 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 будет выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **LDAP-подключение**.

   Отобразится таблица LDAP-подключений.

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

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

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

6. В поле **Альтернативное имя 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 должен использовать 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 должен использовать для поиска учетных записей пользователей в директории удаленного сервера:

   - **uid (OpenLDAP)** – идентификатор пользователя UID (user ID) для поиска в OpenLDAP. Значение 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 котором 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 просмотреть введенный пароль, нажав на значок просмотра 👁.

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

13. 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 будет выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **LDAP-подключение**.

   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 будет выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.
2. Выберите вкладку **LDAP-подключение**.

   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

Таблица пользователей отображается 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.

- **Группы** – группа пользователя.

- **Состояние** – статус пользователя:

  - **В сети**.

  - **Не в сети**.

  - **Заблокирован**.

- **Двухфакторная аутентификация** – статус двухфакторной аутентификации 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 инструкции 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 будет выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

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

3. В отобразившейся области настройки в раскрывающемся списке **Источник** выберите тип пользователя:

   - **Локальный** – значение по умолчанию. При выборе этого значения в полях **Пароль** и **Подтверждение пароля** введите пароль пользователя. Пароль должен содержать как минимум один прописной и строчный символ A–Z, цифру и специальный символ. Длина пароля: от 8 до 50 символов. Вы можете просмотреть введенный пароль, нажав на значок просмотра 👁.

   - **LDAP**.

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**.

6. Если вы хотите включить двухфакторную аутентификацию для пользователя, установите флажок **Двухэтапная аутентификация**. По умолчанию флажок снят. 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.

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

8. Если вы хотите, чтобы при каждом действии пользователя создавался запрос на подтверждение, установите флажок **Требуется подтверждение запроса**. По умолчанию флажок снят, 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, выполнив следующие действия:

    a. В поле **Email** 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 этому пользователю доступ к веб-интерфейсу оркестратора.

Разблокировка и блокировка пользователя

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

Чтобы разблокировать или заблокировать пользователя:

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

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

2. Нажмите на пользователя, которого вы хотите изменить.

3. В отобразившейся области настройки в раскрывающемся списке **Роль** выберите роль пользователя:

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

4. Включите или выключите двухфакторную аутентификацию для пользователя, выполнив одно из следующих действий:

   - Если вы хотите включить двухфакторную аутентификацию для пользователя, установите флажок **Двухэтапная аутентификация**. 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.

   - Если вы хотите выключить двухфакторную аутентификацию для пользователя, снимите флажок **Двухэтапная аутентификация**.

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

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

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

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

9. При необходимости укажите дополнительную информацию о пользователе, выполнив следующие действия:

   a. В поле **Email** введите адрес электронной почты.

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

10. 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 ранее созданного локального пользователя, в меню перейдите в раздел **Пользователи**, нажмите на локального пользователя и в верхней части отобразившейся области настройки 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 один прописной и строчный символ A–Z, цифру и специальный символ. Длина пароля: от 8 до 50 символов. Вы можете просмотреть 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 этот пользователь потерял 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 будет 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** → **Повторно инициализировать двухэтапную аутентификацию**.

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 будет 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

Таблица групп LDAP-пользователей отображается в разделе **Пользователи**. 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 в группе.

Действия, которые вы можете выполнить с таблицей, описаны в инструкции 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.

Чтобы создать группу LDAP-пользователей:

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

   Отобразится страница управления пользователями. По умолчанию будет 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. Если вы хотите назначить право доступа группе LDAP-пользователей, в раскрывающемся списке **Права доступа** выберите ранее созданное право доступа. 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 **Двухэтапная аутентификация**. По умолчанию флажок снят. 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 будет 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 в раскрывающемся списке **Роль** выберите роль LDAP-пользователей в группе:

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

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

6. Включите или выключите двухфакторную аутентификацию для группы LDAP-пользователей, выполнив одно из следующих действий:

- Если вы хотите включить двухфакторную аутентификацию для группы LDAP-пользователей, установите флажок **Двухэтапная аутентификация**. 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. Если вы выключаете двухфакторную аутентификацию для группы LDAP-пользователей, LDAP-пользователи перестают отображаться в таблице пользователей.

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

- Если вы хотите выключить двухфакторную аутентификацию для группы LDAP-пользователей, снимите флажок **Двухэтапная аутентификация**.

7. 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 будет 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 LDAP-групп. 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 будет выбрана вкладка **Пользователи**, на которой отображается таблица пользователей.

2. Выберите вкладку **Проверка подлинности**.

3. Выполните одно из следующих действий:

   - Если вы хотите включить двухфакторную аутентификацию для всех пользователей, установите флажок **Двухэтапная 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 **Двухэтапная аутентификация для всех пользователей**.

   По умолчанию флажок установлен.

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 инструкции Работа с таблицами компонентов решения.

2. 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.

Ограничение продолжительности пользовательского сеанса

По умолчанию если пользователь бездействует на протяжении 3600 секунд (одного часа) после входа в веб-интерфейс оркестратора, пользовательский сеанс прекращается. Вы можете вручную указать время возможного бездействия.

Чтобы ограничить продолжительность пользовательского сеанса:

1. В нижней части меню нажмите на значок настройки → **Время истечения сессии**.
2. В открывшемся окне введите время в секундах, по истечении которого вы хотите прекращать пользовательский сеанс при бездействии. Диапазон значений: от 60 до 86 400. По умолчанию указано значение `3600`.
3. Нажмите на кнопку **Сохранить**.

Пользователи будут автоматически выходить из веб-интерфейса оркестратора при бездействии по истечении указанного времени.

Просмотр и завершение активных пользовательских сеансов

Вы можете просматривать список сеансов, в которых использовалась ваша учетная запись, а также завершать эти сеансы.

Чтобы просмотреть или завершить активные пользовательские сеансы:

1. В нижней части меню нажмите на значок настройки → **Активные сессии**.

   Отобразится таблица активных 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 инструкции Работа с таблицами компонентов решения.

2. Завершите пользовательские сеансы одним из следующих способов:

   - Если вы хотите завершить отдельный пользовательский сеанс, нажмите рядом с ним на кнопку **Закончить сессию**.

   - Если вы хотите завершить несколько пользовательских сеансов, установите рядом с ними флажки и в верхней части таблицы нажмите на кнопку **Действия** → **Закончить сессию**.

Пользовательские сеансы будут завершены.

Управление ресурсами организации

Ресурсы вашей организации объединяются в логические группы – *центры обработки данных* (далее также ЦОД) для последующего управления. Центры обработки данных объединяются в более абстрактные логические группы – *домены*. Вы можете перемещать центры обработки данных между доменами.

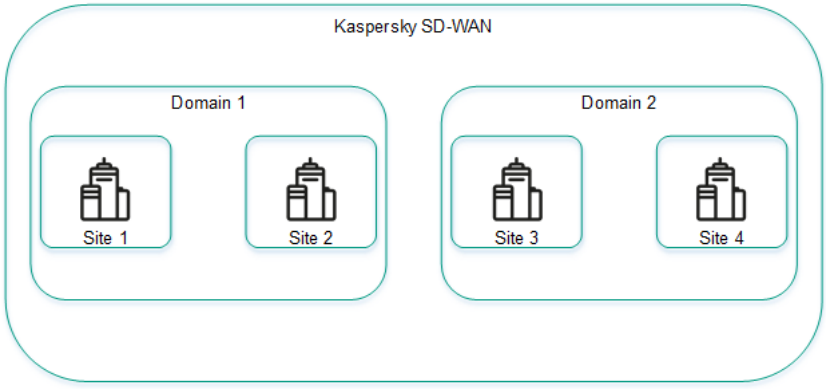
> В Kaspersky SD-WAN термины *центр обработки данных* и *домен* используются в уникальном смысле. Центр обработки данных обозначает группу ресурсов, а не площадку, на которой располагаются и поддерживаются компьютерные системы, серверы и оборудование. Домен обозначает группу центров обработки данных, а не группу компьютеров, серверов и ресурсов в интернете.

В центры обработки данных помещаются следующие ресурсы:

- контроллеры SD-WAN и SDN;
- менеджеры виртуальной инфраструктуры (VIM);
- серверы Zabbix-прокси;
- менеджеры виртуальных сетевых функций (VNFM);
- подсети управления устройствами CPE и виртуальными сетевыми функциями.

Вам нужно создать в каждом центре обработки данных хотя бы одну подсеть управления для назначения IP-адресов устройствам CPE и виртуальным сетевым функциям. Вы также можете указать для виртуальных сетевых функций DNS-серверы и статические маршруты.

На рисунке ниже изображены четыре логические группы ресурсов организации (Site 1, Site 2, Site 3 и Site 4), объединенные в две общие группы (Domain 1 и Domain 2).



Центры обработки данных и домены

Работа с доменами

Список доменов отображается 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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

3. В открывшемся окне в поле **Имя** введите имя домена. Диапазон значений: от 1 до 50 символов.

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

5. Нажмите на кнопку **Создать**.

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

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

Изменение домена

Чтобы изменить домен:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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

3. В открывшемся окне в поле **Имя** введите имя домена. Диапазон значений: от 1 до 50 символов.

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

5. Нажмите на кнопку **Сохранить**.

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

Удаление домена

Удаленные домены невозможно восстановить.

Чтобы удалить домен:

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

Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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.

Создание центра обработки данных

Чтобы создать центр обработки данных:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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

3. В открывшемся окне в поле **Имя** введите имя центра обработки данных. Диапазон значений: от 1 до 50 символов.

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

5. В раскрывающемся списке **Домен** выберите ранее созданный домен, в который вы хотите добавить центр обработки данных.

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

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

8. Нажмите на кнопку **Создать**.

Центр обработки данных будет создан 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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

3. В открывшемся окне в поле **Имя** введите имя центра обработки данных. Диапазон значений: от 1 до 50 символов.

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

5. Если вы хотите развертывать виртуальные сетевые функции и запускать скрипты на устройствах CPE, в поле **VNFM URL** введите веб-адрес VNFM, к которому должен подключиться оркестратор. Вы можете убедиться в доступности VNFM, нажав на кнопку **Проверить соединение**.

6. При необходимости в поле **Адрес** введите адрес центра обработки данных.

7. Нажмите на кнопку **Сохранить**.

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

Миграция центра обработка данных

Чтобы мигрировать центр обработки данных:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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

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

4. Нажмите на кнопку **Мигрировать**.

Начнется миграция центра обработки данных, по завершении которой он отобразится под новым доменом в панели **Ресурсы**.

Удаление центра обработки данных

Удаленные центры обработки данных невозможно восстановить.

Чтобы удалить центр обработки данных:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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 отображения таблицы подсетей управления вам нужно в меню перейти в раздел **Инфраструктура**, нажать на ранее созданный центр обработки данных и выбрать вкладку **IPAM** → **Подсеть**. 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-адрес шлюза, который подсеть управления должна назначать виртуальным сетевым функциям.
- **Диапазон IP** – начальное и конечное значение диапазона, из которого подсеть управления должна назначать IP-адреса устройствам CPE и виртуальным сетевым функциям.
- **DNS** – IPv4-адрес DNS-сервера, который подсеть управления должна назначать виртуальным сетевым функциям.
- **Статические маршруты** – IPv4-адреса источника и назначения статического маршрута, который подсеть управления должна назначать виртуальным сетевым функциям.
- **Использование** – количество IP-адресов, которые подсеть управления назначила устройствам CPE и виртуальным сетевым функциям.

Таблица устройств CPE и виртуальных сетевых функций, которым подсеть управления назначила IP-адреса, отображается на вкладке **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** – тип компонента, которому подсеть управления назначила IP-адрес:
  - **VNF**.
  - **CPE**.
- **Тенант** – тенант, которому назначено устройство CPE или 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. В панели **Ресурсы** выберите ранее созданный домен и центр обработки данных, в которые вы хотите добавить подсеть управления.

3. Выберите вкладку **IPAM**.

   Отобразится 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** – значение по умолчанию.
   - **IPv6**.

7. В поле **CIDR** введите IPv4-адрес и 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, из которого подсеть управления должна назначать IP-адреса устройствам CPE и виртуальным сетевым функциям, выполнив следующие действия:

   a. В блоке **Диапазон IP** нажмите на кнопку **+ Добавить**,

   b. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

   Диапазон IP-адресов будет указан и отобразится в блоке **Диапазон IP**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав рядом с ним на значок удаления ✕.

10. Укажите DNS-сервер, который подсеть управления должна назначать виртуальным сетевым функциям, выполнив следующие действия:

    a. В блоке **DNS** нажмите на кнопку **+ Добавить**.

    b. 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 сервер, нажав рядом с ним на значок удаления ✕.

11. Укажите статический маршрут, который подсеть управления должна назначать виртуальным сетевым функциям, выполнив следующие действия:

    a. В блоке **Статические маршруты** нажмите на кнопку **+ Добавить**.

b. 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 маршрут, нажав рядом с ним на значок удаления ✕.

12. Нажмите на кнопку **Создать**.

Подсеть управления будет создана и отобразится в таблице.

Изменение подсети управления

Вы не можете изменить домен и центр обработки данных, которые вы выбрали при создании подсети управления.

Чтобы изменить подсеть управления:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. В панели **Ресурсы** выберите ранее созданный домен и центр обработки данных, в которые вы добавили подсеть управления.

3. Выберите вкладку **IPAM**.

   Отобразится таблица подсетей управления.

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

5. В открывшемся окне в поле **Имя** введите имя подсети управления.

6. В раскрывающемся списке **Версия IP** выберите версию IP-адресов в подсети управления:

   - **IPv4** – значение по умолчанию.
   - **IPv6**.

7. В поле **CIDR** введите IPv4-адрес и 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, из которого подсеть управления должна назначать IP-адреса устройствам CPE и виртуальным сетевым функциям, выполнив следующие действия:

   a. В блоке **Диапазон IP** нажмите на кнопку **+ Добавить**,

   b. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

   Диапазон IP-адресов будет указан и отобразится в блоке **Диапазон IP**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав рядом с ним на значок удаления ✕.

10. Укажите DNS-сервер, который подсеть управления должна назначать виртуальным сетевым функциям, выполнив следующие действия:

a. В блоке **DNS** нажмите на кнопку **+ Добавить**.

b. 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 сервер, нажав рядом с ним на значок удаления ✕.

11. Укажите статический маршрут, который подсеть управления должна назначать виртуальным сетевым функциям, выполнив следующие действия:

    a. В блоке **Статические маршруты** нажмите на кнопку **+ Добавить**.

    b. 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 маршрут, нажав рядом с ним на значок удаления ✕.

12. Нажмите на кнопку **Сохранить**.

Подсеть 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. В панели **Ресурсы** выберите ранее созданный домен и центр обработки данных, в которые вы добавили подсеть управления.

3. Выберите вкладку **IPAM**.

   Отобразится 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 SD-WAN и SDN

Для отображения таблицы контроллеров вам нужно в меню перейти в раздел **Инфраструктура**, нажать на ранее 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.
- **Узлы контроллера** – IP-адреса узлов контроллера.
- **Тип подключения** – тип подключения устройств CPE к контроллеру:
  - **Unicast**.
  - **Multicast**.
- **Статус кластера** – статус кластера узлов контроллера:
  - **UP** – кластер работает в штатном режиме.
  - **DEGRADED** – при работе кластера возникла ошибка.
  - **DOWN** – кластер не работает.
- **Статус узлов** – статус узлов контроллера:
  - **Подключен (основной)** – узел подключен к контроллеру и является основным в кластере.
  - **Подключен (единственный)** – узел подключен к контроллеру и является единственным в кластере.
  - **Подключен (второстепенный)** – узел подключен к контроллеру и является второстепенным в кластере.
  - **Отключен** – узел не подключен к контроллеру.
  - **Не в кластере** – узел не добавлен в кластер.
  - **Недоступен** – узел недоступен.
  - **Неизвестно** – статус узла неизвестен.

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

Изменение контроллера

Чтобы изменить контроллер:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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 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, выполнив следующие действия:

   a. В поле **Адрес (IP 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. Нажмите на кнопку **Сохранить**.

Контроллер будет изменен и обновится в таблице.

Переход в меню настройки контроллера

Чтобы перейти в меню настройки контроллера:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, в меню настройки которого вы хотите перейти.

Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

Перезагрузка контроллера

Изменения, которые вы вносите в параметры контроллера, могут требовать его перезагрузки (англ. reprovisioning), чтобы вступить в силу. При перезагрузке свойства контроллера 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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.

Скачивание файла с параметрами контроллера

Вы можете скачать файл с параметрами контроллера, чтобы при необходимости восстановить контроллер с помощью этого файла.

Чтобы скачать файл с параметрами контроллера:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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

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

Восстановление контроллера

Чтобы восстановить контроллер:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Восстановить** рядом с контроллером, который вы хотите восстановить.

3. В открывшемся окне укажите путь к ранее скаченному файлу с параметрами контроллера.

4. Нажмите на кнопку **Восстановить**.

Параметры контроллера будут изменены в соответствии с параметрами файла.

Удаление контроллера

Удаленные контроллеры невозможно восстановить.

Чтобы удалить контроллер:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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 просмотреть таблицу всех или изменяемых свойств контроллера:

- Для отображения таблицы всех свойств контроллера вам нужно в меню перейти в раздел **Инфраструктура**, нажать на ранее созданный центр обработки данных, выбрать вкладку **Сетевые ресурсы** и нажать на кнопку **Управление** → **Свойства** рядом с контроллером.
- Для отображения таблицы изменяемых свойств контроллера вам нужно в меню перейти в раздел **Инфраструктура**, нажать на ранее созданный центр обработки данных, выбрать вкладку **Сетевые ресурсы**, нажать на кнопку **Управление** → **Свойства** рядом с контроллером и на открывшейся странице 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 инструкции 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.

- `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`

  Начальный номер порта в диапазоне портов коммутаторов. В диапазон добавляются порты с тремя следующими по порядку номерами. Например, если вы вводите `6553`, в диапазон входят порты с номерами 6553, 6554, 6555, 6556.

- `controller.sockets.config.nodelay`

  Требуется ли включить опцию TCP_NODELAY для управляющих сессий между коммутаторами и контроллером. Возможные значения: `true` или `false`.

- `controller.sockets.mode.epoll`

  Должен ли контроллер использовать систему epoll при работе с коммутаторами. Возможные значения: `true` или `false`.

- `controller.sockets.timeouts.idle.both`

  Время в миллисекундах, по прошествии которого управляющие сессии между коммутаторами и контроллером должны переходить 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, по прошествии которого управляющие сессии между коммутаторами и контроллером должны переходить в состояние ожидания при отсутствии операций чтения. Отсчет времени начинается заново при каждом выполнении операции чтения.

- `controller.sockets.timeouts.idle.write`

  Время в миллисекундах, по прошествии которого управляющие сессии между коммутаторами и контроллером должны переходить в состояние ожидания при отсутствии операций записи. Отсчет времени начинается заново при каждом выполнении операции записи.

- `controller.threads.affinity`

  Должны ли потоки Netty предпочтительно запускаться на разных ядрах центральных процессоров для разных коммутаторов. Возможные значения: `true` или `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, по прошествии которого на коммутаторах должны удаляться flow-правила, автоматически созданные контроллером при обработке первого перехваченного пакета трафика для блокировки последующих пакетов. Отсчет времени начинается заново при каждом применении flow-правила.

- `core.link.bonding.enable`

  Требуется ли включить объединение (англ. bonding) параллельных каналов между двумя коммутаторами. Возможные значения: `true` или `false`.

- `core.link.bonding.equal.cost`

  Требуется ли использовать алгоритм equal cost при объединении каналов. Возможные значения: `true` или `false`. Если вы указываете значение `false`, используется алгоритм unequal cost.

- `core.link.bonding.max.links`

  Максимальное количество каналов в объединенном канале.

- `core.link.bonding.mode`

  Тип группы объединенных каналов. Возможные значения:

  - `BALANCING` – трафик распределяется по каналам в соответствии со значением хеша. Хеш подсчитывается на основании полей IP Proto, IP src-dst и Port src-dst пакетов трафика.

  - `BROADCAST` – трафик дублируется во все каналы.

- `core.link.check.ports.status`

  Должен ли контроллер для обнаружения каналов между коммутаторами периодически отправлять LLDP-пакеты только на включенные (англ. enabled) порты. Возможные значения: `true` или `false`.

- `core.link.enabled.ports.only`

  Должны ли коммутаторы пересылать LLDP-пакеты контроллеру только со включенных портов, когда контроллер пытается обнаружить каналы между коммутаторами. Возможные значения: `true` или `false`.

- `core.link.liveness.interval`

  Интервал в миллисекундах для отправки контроллером LLDP-пакетов по каналам коммутаторов.

- `core.link.liveness.timeout`

  Интервал в миллисекундах для получения и пересылки контроллеру LLDP-пакетов с приемной стороны каналов коммутаторов. Если в течение указанного времени по каналу не поступает LLDP-пакетов, контроллер считает канал недоступным.

- `core.lldp.sendrem.enabled`

  Должны ли коммутаторы отправлять контроллеру уведомления при удалении flow-правил, которые отправляют пакеты трафика на этот контроллер. Возможные значения: `true` или `false`.

- `core.switch.liveness.interval`

  Интервал в миллисекундах для проверки подключения коммутаторов к контроллеру.

- `core.switch.liveness.timeout`

  Время в миллисекундах, в течение которого отключенные коммутаторы должны повторно подключиться к контроллеру.

- `core.tunnel.port.end`

  Конечный номер виртуального сетевого интерфейса (англ. virtual network interface, VNI) в диапазоне интерфейсов коммутаторов.

- `core.tunnel.port.start`

  Начальный номер виртуального сетевого интерфейса в диапазоне интерфейсов коммутаторов.

- `dampening.link.enabled`

  Требуется ли включить функцию Dampening на каналах. Возможные значения: `true` или `false`.

- `dampening.link.maxSuppressTime.ms`

  Максимальное время в миллисекундах, в течение которого доступ к каналу может быть ограничен. По истечении указанного времени счетчики функции Dampening сбрасываются.

- `dampening.link.penalty`

  Число, которое должно прибавляться к показателю Penalty при изменении состояния канала.

- `dampening.link.suppressLevel`

  Значение показателя Penalty, при котором доступ к каналу должен быть ограничен.

- `dampening.link.updateInterval.ms`

  Время в миллисекундах, в течение которого показатель Penalty должен набрать значение свойства `dampening.link.suppressLevel`, чтобы доступ к каналу был ограничен.

- `eth.s.type`

  Значение IEEE 802.1Q TPID, которое устанавливается как внутренняя метка для пакетов трафика с инкапсуляцией Q-in-Q.

- `eth.t.type`

  Значение IEEE 802.1Q TPID, которое устанавливается как внешняя метка для пакетов трафика с инкапсуляцией Q-in-Q.

- `inband.statistics.enabled`

  Требуется ли включить получение статистики на коммутаторах. Статистика содержит информацию сетевых устройствах, к которым подключен коммутатор, а также об используемых портах. Возможные значения: `true` или `false`.

- `inband.swos.cookie`

  Значение поля cookie в сообщении запроса статистики с коммутаторов. Вам нужно указать значение для этого свойства, 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 должны быть заблокированы после попытки подключиться к контроллеру с неверным TLS-сертификатом.

- `openflow.fail2ban.enabled`

  Требуется ли блокировать IP-адреса и порты коммутаторов после попытки подключиться к контроллеру с неверным TLS-сертификатом. Возможные значения: `enabled` или `disabled`.

- `openflow.fail2ban.findTimeSec`

  Время в секундах, в течение которого коммутаторы должны совершить количество попыток подключения к контроллеру с неверным TLS-сертификатом, указанное в свойстве `openflow.fail2ban.maxRetry`, 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 этих коммутаторов должны быть заблокированы.

- `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`

  Требуется ли разрешить flow-правилам отправлять пакеты трафика на контроллер. Возможные значения: `true` или `false`.

- `openflow.io.rate.limiter.switch.type-to-rate`

  Это свойство больше не используется.

- `openflow.io.switch.latency.monitoring.delay.ms`

  Интервал в миллисекундах для проверки задержки между контроллером и коммутаторами.

- `openflow.io.switch.latency.monitoring.enabled`

  Требуется ли включить проверку задержки между контроллером и коммутаторами. Возможные значения: `true` или `false`.

- `openflow.io.switch.latency.sma.initial.drop.size`

  Количество начальных пакетов трафика на коммутаторах, которые не должны использоваться при подсчете статистики.

- `openflow.io.switch.latency.sma.window.size`

  Количество последних пакетов трафика на коммутаторах, которые должны использоваться 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 транспортных путей в сегменте.

- `segment.path.spf.num.max`

  Максимальное количество транспортных путей SPF для автоматической балансировки.

- `table-miss.mode`

  Действие, которое коммутаторы должны выполнять 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`

  Требуется ли использовать Connectivity Fault Management (CFM) на каналах. Возможные значения: `true` или `false`.

- `topology.debug.enabled`

  Требуется ли включить использование процедур отладки контроллера с помощью протокола gRPC. Возможные значения: `true` или `false`.

- `topology.intervtep.links.enabled`

  Требуется ли разрешить построение каналов между VTEP. Возможные значения: `true` или `false`.

- `topology.link.charged`

  Требуется ли использовать все каналы в последнюю очередь при маршрутизации трафика независимо от качества связи. Возможные значения: `true` или `false`.

- `topology.link.discovery.groups.enabled`

  Требуется ли разрешить обнаружение каналов по группам.

- `topology.link.encryption.enabled`

  Требуется ли включить шифрование трафика на каналах. Возможные значения: `true` или `false`.

- `topology.link.encryption.key.update.interval.minutes`

  Интервал в минутах для обновления ключа дешифровки на каналах.

- `topology.link.error.monitoring.enabled`

  Требуется ли включить мониторинг ошибок на каналах. Возможные значения: `true` или `false`.

- `topology.link.error.threshold.eps`

  Пороговое значение количества ошибок в секунду на каналах.

- `topology.link.eu.monitoring.delay.sec`

  Интервал в секундах для измерения количества ошибок на каналах и загруженности каналов.

- `topology.link.fec.enable`

  Требуется ли включить функцию Forward Error Correction (FEC) на каналах. Возможные значения: `true` или `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`

  Требуется ли включить мониторинг джиттера на каналах. Возможные значения: `true` или `false`.

- `topology.link.jitter.threshold.ms`

  Пороговое значение времени джиттера в миллисекундах на каналах.

- `topology.link.latency.monitoring.enabled`

  Требуется ли включить мониторинг задержек на каналах. Возможные значения: `true` или `false`.

- `topology.link.latency.threshold.ms`

  Пороговое значение времени задержки в миллисекундах на каналах.

- `topology.link.ljp.monitoring.delay.sec`

  Интервал в секундах для сравнения полученных показателей мониторинга с указанными пороговыми значениями задержек, джиттера и потери пакетов на каналах.

- `topology.link.ljp.stats.collecting.enabled`

  Требуется ли включить мониторинг задержек, джиттера и потерь пакетов трафика на каналах. Возможные значения: `true` или `false`. Вы можете указать протокол для мониторинга 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 каналах. Вам нужно указать значение для этого свойства, 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 каналах. Возможные значения: `LLDP` или `GENEVE`.

- `topology.link.ljp.stats.collecting.multiplicity`

  Множитель, который должен применяться на контроллере к показателям мониторинга задержек, джиттера и потерь пакетов трафика на каналах. Вам нужно указать значение для этого свойства, если для свойства `topology.link.ljp.stats.collecting.method` вы указали значение `GENEVE`.

- `topology.link.packet.loss.monitoring.enabled`

  Требуется ли включить мониторинг потерь пакетов трафика на каналах. Возможные значения: `true` или `false`.

- `topology.link.packet.loss.threshold.percents`

  Пороговое значение процента потерь пакетов трафика на каналах.

- `topology.link.pmtud.scheduler.interval.sec`

  Интервал в секундах для автоматического повторного определения показателя MTU на каналах.

- `topology.link.pmtud.wait.time.ms`

  Время в миллисекундах для ожидания контроллером пакета PMTUD LLDP. Если по прошествии этого времени контроллер не получает пакет PMTUD LLDP, контроллер считает, что пакет такого размера невозможно передать по каналу.

- `topology.link.threshold.monitoring.delay.sec`

  Интервал в секундах для мониторинга пороговых значений на каналах.

- `topology.link.threshold.monitoring.enabled`

  Требуется ли включить мониторинг пороговых значений на каналах. Возможные значения: `true` или `false`.

- `topology.link.threshold.monitoring.unban.periods`

  Количество успешных проверок подряд для разблокирования каналов. Проверка проводится раз в секунду.

- `topology.link.util.monitoring.enabled`

  Требуется ли включить мониторинг загруженности (использования полосы) каналов. Возможные значения: `true` или `false`.

- `topology.link.util.threshold.percents`

  Пороговое значение загруженности каналов в процентах от скорости сервисных интерфейсов.

- `topology.overlay.lldp.sender.concurrent`

  Должен ли контроллер параллельно отправлять LLDP-пакеты для обнаружения каналов. Возможные значения: `true` или `false`.

- `topology.overlay.lldp.sender.core.pool.size`

Минимальное количество потоков для параллельной отправки контроллером LLDP-пакетов. Вам нужно указать значение для этого свойства, 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. Вам нужно указать значение для этого свойства, 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. Вам нужно указать значение для этого свойства, если для свойства `topology.overlay.lldp.sender.concurrent` вы указали значение `true`.

- `topology.reserve.si.auto.revert.enabled`

  Должен ли резервный сервисный интерфейс снова стать резервным, если прежний сервисный интерфейс восстанавливает работу. Возможные значения: `true` или `false`.

- `topology.throttler.timeout.hard.enabled`

  Требуется ли накапливать на контроллере физические операции, такие как подключение коммутатора или порта, и выполнять их по прошествии указанного вами времени. Вы можете указать время с помощью свойств `topology.throttler.timeout.hard.ms` и `topology.throttler.timeout.idle.ms`. Возможные значения: `true` или `false`.

- `topology.throttler.timeout.hard.ms`

  Время в секундах, по прошествии которого выполняются накопившиеся на контроллере физические операции. Вам нужно указать значение для этого свойства, если для свойства `topology.throttler.timeout.hard.enabled` вы указали значение `true`.

- `topology.throttler.timeout.idle.ms`

  Время в секундах, по прошествии которого выполняются накопившиеся на контроллере физические операции. Отсчет времени начинается заново при каждом появлении физической операции. Вы можете указать значение для этого свойства, 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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

   Откроется страница управления свойствами контроллера. По умолчанию будет 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**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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 будет 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.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

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

   Откроется страница управления свойствами контроллера. По умолчанию будет 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.

Просмотр информации об узлах контроллера

Чтобы просмотреть информацию об узлах контроллера:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, информацию об узлах которого вы хотите просмотреть.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** – статус узла контроллера:
  - **Подключен (основной)** – узел подключен к контроллеру и является основным в кластере.
  - **Подключен (единственный)** – узел подключен к контроллеру и является единственным в кластере.
  - **Подключен (второстепенный)** – узел подключен к контроллеру и является второстепенным в кластере.
  - **Отключен** – узел не подключен к контроллеру.
  - **Не в кластере** – узел не добавлен в кластер.
  - **Недоступен** – узел недоступен.
  - **Неизвестно** – статус узла неизвестен.
- **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 инструкции Работа с таблицами компонентов решения.

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

Работа с VIM

Вы можете развернуть VIM на одной из ваших площадок или на устройстве uCPE. Развертывание VIM на площадке, подразумевает централизованное управление жизненным циклом виртуальных сетевых функций. Развертывание VIM на устройстве uCPE позволяет доставлять виртуальные сетевые функции на удаленные площадки и управлять этими функциями локально.

Для отображения таблицы VIM вам нужно в меню перейти в раздел **Инфраструктура**, нажать на ранее 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 используется VIM от облачной платформы OpenStack.
- **Функция** – развернут ли VIM в центре обработки данных или на устройстве uCPE.
- **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** – находится ли VIM за NAT (Network Address Translation).

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

Настройка VIM, развернутого на площадке

Чтобы настроить VIM, развернутый на площадке:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. В панели **Ресурсы** выберите ранее созданный домен и центр обработки данных, к которым относится площадка.

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 сервису идентификации VIM. По умолчанию указано значение `5000`.

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

   - **http** – значение 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 проходит успешно, оркестратор получает доступ к управлению доступной администратору виртуальной инфраструктурой.

10. Укажите дополнительные параметры аутентификации оркестратора в облачной платформе OpenStack, выполнив следующие действия:

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

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

11. 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 трансляция сетевых адресов.
    - **Выключено** – VIM не находится за NAT. Это значение выбрано по умолчанию.

12. Укажите коэффициенты переподписки физических ресурсов, выполнив следующие действия:

    a. В поле **Переподписка ЦП** введите коэффициент переподписки ядер процессора. По умолчанию указано значение `1`.

    b. В поле **Переподписка ОЗУ** введите коэффициент переподписки оперативной памяти. По умолчанию указано значение `1`.

    c. В поле **Переподписка диска** введите коэффициент переподписки дискового пространства. По умолчанию указано значение `1`.

    Коэффициенты переподписки позволяют предоставлять виртуальным машинам больше виртуальных ресурсов, чем доступно физических. Это возможно потому, что как правило 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. По умолчанию указано значение `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, или значение **Отсутствует**, если OpenStack не подключен к SDN-кластеру.

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 идентификатор VLAN-тег.

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

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 интерфейсов** 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, выполнив следующие действия:

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 sercurity:

- **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 этого VIM в шаблоне uCPE. Когда вы указываете параметры VIM в шаблоне uCPE, эти параметры распространяются на все использующие шаблон устройства.

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 будет 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 сервису идентификации VIM. По умолчанию указано значение `5000`.

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

   - **http** – значение 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, выполнив следующие действия:

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

   b. В поле **Домен** введите имя OpenStack-домена для аутентификации оркестратора в этом 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. Значение по умолчанию.

10. Укажите коэффициенты переподписки физических ресурсов, выполнив следующие действия:

    a. В поле **Переподписка ЦП** введите коэффициент переподписки ядер процессора. По умолчанию указано значение `1`.

    b. В поле **Переподписка ОЗУ** введите коэффициент переподписки оперативной памяти. По умолчанию указано значение `1`.

    c. В поле **Переподписка диска** введите коэффициент переподписки дискового пространства. По умолчанию указано значение `1`.

Коэффициенты переподписки позволяют предоставлять виртуальным машинам больше виртуальных ресурсов, чем доступно физических. Это возможно потому, что как правило 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

Чтобы изменить VIM:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. В панели **Ресурсы** выберите ранее созданный домен и центр обработки данных, к которым относится 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 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 сервису идентификации VIM. По умолчанию указано значение `5000`.

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

   - **http** – значение 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 проходит успешно, оркестратор получает доступ к управлению доступной администратору виртуальной инфраструктурой.

10. Укажите дополнительные параметры аутентификации оркестратора в облачной платформе OpenStack, выполнив следующие действия:

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

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

11. 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 трансляция сетевых адресов.
    - **Выключено** – VIM не находится за NAT. Это значение выбрано по умолчанию.

12. Укажите коэффициенты переподписки физических ресурсов, выполнив следующие действия:

    a. В поле **Переподписка ЦП** введите коэффициент переподписки ядер процессора. По умолчанию указано значение `1`.

    b. В поле **Переподписка ОЗУ** введите коэффициент переподписки оперативной памяти. По умолчанию указано значение `1`.

    c. В поле **Переподписка диска** введите коэффициент переподписки дискового пространства. По умолчанию указано значение `1`.

    Коэффициенты переподписки позволяют предоставлять виртуальным машинам больше виртуальных ресурсов, чем доступно физических. Это возможно потому, что как правило 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. По умолчанию указано значение `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, или значение **Отсутствует**, если OpenStack не подключен к SDN-кластеру.

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 идентификатор VLAN-тег.

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

    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 интерфейсов** 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, выполнив следующие действия:

    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 sercurity:

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

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

20. Нажмите на кнопку **Сохранить**.

VIM будет изменен и обновится в таблице.

Просмотр использования VIM

Вы можете просмотреть, насколько VIM использует следующие вычислительные ресурсы:

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

Чтобы просмотреть использование VIM:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. В панели **Ресурсы** выберите ранее созданный домен и центр обработки данных, к которым относится VIM.

3. Выберите вкладку **Вычислительные ресурсы**.

   Отобразится таблица VIM.

4. Нажмите на кнопку **Управление** → **Показать использование** рядом с VIM, использование которого вы хотите просмотреть.

Откроется окно с информацией об использовании VIM вычислительных ресурсов.

Удаление VIM

Удаленные VIM невозможно восстановить.

Чтобы удалить VIM:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. В панели **Ресурсы** выберите ранее созданный домен и центр обработки данных, к которым относится 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.

Мультитенантность

Kaspersky SD-WAN является *мультитенантным* решением, компоненты которого вы можете разделить между несколькими *тенантами* – независимыми клиентами, офисами или подразделениями вашей организации. Каждый тенант имеет собственный экземпляр SD-WAN и портал самообслуживания. Тенанты изолированы и не могут получить доступ к порталам самообслуживания друг-друга, но могут использовать общую подсеть управления.

Список тенантов отображается в разделе **Тенанты**. В этом разделе также отображаются следующие блоки для назначения тенанту компонентов решения и просмотра информации о тенантах:

- **VIM** – для назначения тенантам VIM.
- **Группы пользователей** – для назначения тенанту групп пользователей.
- **Каталог** – для назначения тенанту компонентов сетевого сервиса.
- **Сервис SD-WAN** – для просмотра компонентов сервиса SD-WAN тенанта.
- **Ресурсы** – для назначения вычислительных ресурсов тенанту.
- **Сервисные запросы** – для просмотра сервисных запросов тенанта.
- **Пользователи** – для назначения тенанту пользователей.
- **Устройства CPE** – для добавления тенанту устройств CPE.

Создание тенанта

Чтобы создать тенанта:

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

   Отобразится страница управления тенантами.

2. Если вы создаете первого тенанта, в блоке **Тенанты** в поле **Имя** введите имя тенанта.
3. Если вы создаете второго или последующих тенантов, выполните следующие действия:

   a. В верхней части блока **Тенанты** нажмите на кнопку **+ Тенант**.

   b. В поле **Имя** введите имя тенанта.

4. При необходимости в блоке в нижней части страницы введите краткое описание тенанта.
5. Нажмите на кнопку создания +

Тенант будет создан и отобразится в блоке **Тенанты**.

Назначение тенанту пользователя

Чтобы назначить тенанту пользователя:

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

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта, которому вы хотите назначить пользователя.

3. В блоке **Пользователи** нажмите на кнопку **+ Изменить**.

4. В открывшемся окне в блоке **Пользователи** выберите ранее созданного пользователя, которого вы хотите назначить тенанту.

   Пользователь отобразится в блоке **Назначить пользователей**.

5. Нажмите на кнопку **Сохранить**.

Пользователь будет назначен тенанту и отобразится в блоке **Пользователи**.

Назначение тенанту группы пользователей

Чтобы назначить тенанту группу пользователей:

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

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта, которому вы хотите назначить группу пользователей.

3. В блоке **Группы пользователей** нажмите на кнопку **+ Изменить**.

4. В открывшемся окне в блоке **Группы** выберите ранее созданную группу пользователей, которую вы хотите назначить тенанту.

   Группа пользователей отобразится в блоке **Назначить группы**.

5. Нажмите на кнопку **Сохранить**.

Группа пользователей будет назначена тенанту и отобразится в блоке **Группы пользователей**.

Назначение тенанту вычислительных ресурсов

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 кнопку 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

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 разделе **Каталог** портала самообслуживания тенанта.

Назначение тенанту VIM

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.
3. В блоке **VIM** нажмите на кнопку **+ Изменить**.
4. В открывшемся окне в блоках **Домен** и **Центр обработки данных** выберите ранее созданный домен и центр обработки данных, в котором развернут VIM.
5. В блоке **VIM** выберите VIM, который вы хотите назначить тенанту.

   VIM отобразится в блоке **Назначить VIM**.
6. Нажмите на кнопку **Сохранить**.

VIM будет назначен тенанту и отобразится в блоке **VIM**.

Вход в портал самообслуживания тенанта

Чтобы войти в портал самообслуживания тенанта:

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

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта, в портал самообслуживания которого вы хотите войти.

3. Нажмите на кнопку **Подключиться как тенант**.

Портал самообслуживания тенанта откроется в новой вкладке браузера и вы войдете в него.

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. В поле **Имя** введите имя тенанта.

4. В блоке в нижней части страницы введите краткое описание тенанта.

5. Нажмите на значок сохранения .

Тенант будет изменен и обновится в блоке **Тенанты**.

Удаление тенанта

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**.

Управление экземплярами SD-WAN

Экземпляр SD-WAN (англ. SD-WAN instance) – это развернутое для тенанта решение Kaspersky SD-WAN. Вы можете настроить экземпляр SD-WAN в соответствии с требованиями организации к необходимым уровням гибкости, безопасности и производительности при передаче данных через WAN.

Вам нужно указать параметры экземпляра SD-WAN в шаблоне, после чего использовать его при развертывании экземпляров SD-WAN для тенантов, чтобы не настраивать каждый отдельный экземпляр. Если вы хотите, чтобы тенант использовал шаблон экземпляра SD-WAN, этого тенанта необходимо добавить в шаблон.

При несовпадении параметров, указанных в шаблоне экземпляра SD-WAN, с фактическими параметрами экземпляра тенанта решение не развертывается. Например, вы можете столкнуться с ошибкой при развертывании решения для тенанта, если в используемом шаблоне экземпляра SD-WAN указано количество узлов контроллера, которое отличается от реального количества узлов у тенанта.

Вы можете сгруппировать экземпляры SD-WAN в пулы для масштабируемости и отказоустойчивости, особенно в условиях использования большого количества устройств CPE. Каждый пул экземпляров SD-WAN является балансировщиком нагрузки, где нагрузкой выступают устройства CPE.

При добавлении устройства CPE его можно назначить пулу экземпляров SD-WAN или отдельным экземплярам из этого пула. Если вы назначаете устройство CPE пулу экземпляров SD-WAN, оркестратор автоматически выбирает из этого пула экземпляр SD-WAN с наименьшим количеством устройств и назначает ему устройство. При совпадении количества устройств CPE экземпляр SD-WAN выбирается случайно.

Работа с шаблонами экземпляра SD-WAN

Таблица шаблонов экземпляра SD-WAN отображается в разделе **SD-WAN → Шаблоны экземпляров SD-WAN**. По умолчанию создан шаблон экземпляра SD-WAN **Default SD-WAN template**. Если тенант, для которого вы развертываете решение, не добавлен ни в один шаблон экземпляра SD-WAN, этот тенант использует шаблон по умолчанию. Информация о шаблонах экземпляра SD-WAN отображается в следующих столбцах таблицы:

- **ID** – идентификатор шаблона экземпляра SD-WAN.
- **Имя** – имя шаблона экземпляра SD-WAN.
- **Используется** – используется ли шаблон 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 инструкции Работа с таблицами компонентов решения.

Параметры шаблона экземпляра SD-WAN отображаются на следующих вкладках:

- **Информация** – основная информация о шаблоне экземпляра SD-WAN. Вы можете изменить имя шаблона в поле **Имя**.
- **Классы трафика** – параметры классов трафика.
- **QoS-правила** – параметры правил качества обслуживания.
- **Транспортные сервисы** – параметры транспортных сервисов.
- **Тенанты** – тенанты, добавленные в шаблон экземпляра SD-WAN.
- **Высокая доступность** – количество узлов контроллера, которое будет развернуто в экземпляре SD-WAN.
- **Транспортная/сервисная стратегия** – используемая транспортная стратегия.

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 **+ Шаблон экземпляра SD-WAN**.
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.

Назначение шаблона 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 по умолчанию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет 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 по умолчанию.

Выбор количества узлов контроллера

Вы можете выбрать, сколько узлов контроллера будет развернуто в экземпляре SD-WAN.

Чтобы выбрать количество узлов контроллера:

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 выбрать количество узлов контроллера.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

3. Выберите вкладку **Высокая доступность**.

4. Выберите количество узлов контроллера SD-WAN.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона экземпляра SD-WAN.

Добавление тенанта в шаблон 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.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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 ранее 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

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.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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

Таблица экземпляров SD-WAN отображается 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** – для экземпляра SD-WAN не развернут контроллер.
  - **Ошибка** – при работе экземпляра SD-WAN возникла ошибка.
  - **Удаление** – экземпляр SD-WAN находится в процессе удаления.
  - **Deleted** – экземпляр SD-WAN удален.
- **Количество CPE** – количество устройств CPE, добавленных экземпляру SD-WAN.
- **Контроллеры** – IP-адреса и номера портов контроллеров, развернутых в экземпляре SD-WAN.
- **ЦОД** – центр обработки данных, в котором развернут экземпляр SD-WAN.
- **VIM** – VIM, развернутый в экземпляре SD-WAN.
- **Создан** – дата и время развертывания экземпляра SD-WAN.

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

Параметры экземпляра SD-WAN отображаются на следующих вкладках:

- **Конфигурация** – основная информация об экземпляре SD-WAN.
- **Мониторинг** – результаты мониторинга экземпляра SD-WAN.
- **Сервисные запросы** – сервисные запросы экземпляра SD-WAN.
- **Самообслуживание тенанта** – тенанты, добавленные в экземпляр SD-WAN.

Просмотр использования экземпляра SD-WAN

Вы можете просмотреть, какие устройства CPE добавлены экземпляру SD-WAN.

Чтобы просмотреть использование 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, использование которого вы хотите просмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет 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 **Устройства CPE**, в котором отображается таблица устройств CPE, добавленных экземпляру SD-WAN.

Переход в меню настройки контроллера, развернутого для экземпляра SD-WAN

Чтобы перейти в меню настройки контроллера, развернутого для 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.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об экземпляре SD-WAN.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Управлять контроллером SD-WAN**.

Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

Переход к топологии сетевого сервиса SD-WAN, развернутого для экземпляра

Чтобы перейти к топологии сетевого сервиса SD-WAN, развернутого для экземпляра:

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

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об экземпляре SD-WAN.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Управлять сетевым сервисом SD-WAN**.

Веб-интерфейс оркестратора экземпляра SD-WAN откроется в новой вкладке браузера, вы автоматически войдете в него и перейдете в раздел **Каталог**. Топология сетевого сервиса SD-WAN отобразится в графическом конструкторе.

Просмотр топологии развернутого экземпляра SD-WAN

Вы можете просмотреть топологию развернутого экземпляра SD-WAN. В топологии отображаются туннели и сегменты между устройствами CPE, а также транспортные пути внутри сегментов.

Чтобы просмотреть топологию развернутого экземпляра SD-WAN:

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

Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, развернутым для экземпляра SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Топология**.

   Отобразится топология экземпляра SD-WAN.

4. При необходимости установите следующие флажки:

   - Установите флажок **Использование туннеля**, чтобы отобразить загруженность туннелей. Уровень загруженности туннеля соответствует следующим цветам:
     - Зеленый – малая загруженность туннеля.
     - Желтый – средняя загруженность туннеля.
     - Красный – высокая загруженность туннеля.
   - Установите флажок **Сегменты** и в раскрывающемся списке **Коммутаторы сегмента** выберите два устройства CPE, чтобы отобразить все туннели между этими устройствами.
   - 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

Вы можете добавить тенанта в развернутый экземпляр SD-WAN. Если тенанты добавлены в один экземпляр SD-WAN, между добавленными этим тенантам устройствами CPE устанавливается связность.

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 будет 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 ранее 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

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 будет 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 для этого экземпляра. 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 будет 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

Таблица пулов экземпляров SD-WAN отображается 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.
- **Количество CPE** – количество устройств CPE, добавленных экземплярам SD-WAN.
- **Создан** – дата и время создания пула экземпляров SD-WAN.

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

Параметры пула экземпляров SD-WAN отображаются на следующих вкладках:

- **Информация** – основная информация о пуле экземпляров SD-WAN. Вы можете изменить имя пула экземпляров в поле **Имя** и ввести его краткое описание в поле **Описание**.
- **Экземпляры SD-WAN** – добавленные в пул экземпляры 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.

Добавление экземпляра SD-WAN в пул

Чтобы добавить экземпляр SD-WAN в пул:

1. В меню перейдите в раздел **SD-WAN → Пулы экземпляров SD-WAN**.

Отобразится таблица пулов экземпляров SD-WAN.

2. Нажмите на пул, 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 будет 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 **+ Экземпляр SD-WAN**.

5. В открывшемся окне выберите ранее развернутый экземпляр SD-WAN, который вы хотите добавить в пул.

6. Нажмите на кнопку **Добавить**.

   Экземпляр SD-WAN будет добавлен в пул и отобразится в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры пула экземпляров SD-WAN.

Удаление экземпляра SD-WAN из пула

Чтобы удалить экземпляр SD-WAN из пула:

1. В меню перейдите в раздел **SD-WAN** → **Пулы экземпляров SD-WAN**.

   Отобразится таблица пулов экземпляров SD-WAN.

2. Нажмите на пул, 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 будет 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.

   Экземпляр SD-WAN будет удален из пула 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

Удаленные пулы 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 будет 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. Вы можете приобрести устройства CPE модели KESR или развернуть их как виртуальные машины с помощью полученного от специалистов "Лаборатории Касперского" образа. При использовании виртуальных машин вам нужно убедиться, что они соответствуют аппаратным требованиям.

Для построения сети SD-WAN, централизованного управления и выполнения основных функций на устройствах CPE установлен виртуальный коммутатор OpenFlow (англ. OpenFlow virtual switch, далее также виртуальный коммутатор, vSwitch). Например, с помощью виртуального коммутатора выполняются настраиваются потоки трафика.

Вам нужно указать параметры в шаблоне CPE, после чего применить его к устройствам при их добавлении или ручной регистрации, чтобы не настраивать каждое отдельное устройство. Если вы изменяете параметр в шаблоне CPE, этот параметр автоматически изменяется на всех использующих шаблон устройствах.

Если вы изменяете параметр на устройстве CPE, этот параметр перестает зависеть от шаблона. При изменении в шаблоне CPE такой параметр не изменяется на устройстве.

> Определенные параметры устройства CPE можно указать только в шаблоне, например номер порта для подключения к оркестратору.

Новые устройства CPE регистрируются автоматически (англ. Zero Touch Provisioing, ZTP). Вы добавляете устройство CPE в веб-интерфейс оркестратора, генерируете веб-адрес с базовыми параметрами и вводите этот адрес на устройстве. Устройство CPE подключается к оркестратору с помощью полученных параметров, сопоставляется с ранее добавленной записью и автоматически регистрируется. Во время регистрации не требуется подключаться к облачным сервисам "Лаборатории Касперского".

Вы можете использовать *двухфакторную аутентификацию*, чтобы безопасно зарегистрировать устройство CPE. При двухфакторной аутентификации в базу данных оркестратора записывается токен (ключ безопасности), который затем вы помещаете на устройство CPE с помощью веб-адреса с базовыми параметрами. Регистрация проходит успешно, если при подключении устройства CPE к оркестратору помещенный на устройство токен совпадает с токеном в базе данных оркестратора.

Когда вы удаляете устройство CPE из веб-интерфейса оркестратора, на устройстве сохраняются базовые параметры. При необходимости в повторной регистрации вам нужно перезагрузить устройство CPE, чтобы оно подключилось к оркестратору и отобразилось в веб-интерфейсе оркестратора, после чего зарегистрировать устройство вручную. Вы не можете использовать двухфакторную аутентификацию при повторной регистрации устройства CPE.

При добавлении и регистрации устройства CPE вы можете выбрать, должно ли оно автоматически включиться (англ. enable) после регистрации. Когда устройство CPE включено, к нему применяется шаблон CPE, и это устройство становится доступным для передачи трафика.

О взаимодействии между устройством CPE и оркестратором

После регистрации устройство CPE отправляет REST API-запросы оркестратору для получения задач, не связанных с управлением виртуальным коммутатором, например для перезагрузки устройства и обновления прошивки. Запросы отправляются с периодичностью, которую вы указываете при настройке подключения устройства CPE к оркестратору и контроллеру.

Для отображения таблицы выполняемых оркестратором задач на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE** и нажать на устройство. 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**.
5. 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 3-х попыток на устройстве указываются предыдущие параметры, а в таблице задача отображается со статусом в **Ошибка**.

О взаимодействии между устройством CPE и контроллером

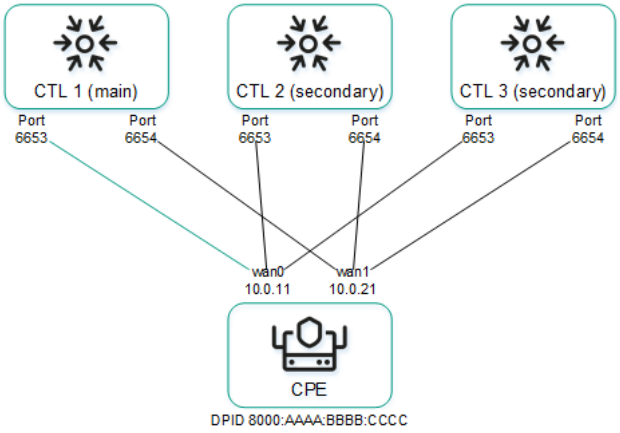
После регистрации устройства CPE между каждым его интерфейсом SD-WAN с типом WAN и доступными контроллерами устанавливается зашифрованная или незашифрованная управляющая сессия. Одна из этих сессий является основной (англ. primary session), а остальные находятся в режиме ожидания.

По основной сессии на устройство CPE передаются задачи, связанные с управлением виртуальным коммутатором, например изменение параметров транспортных путей. Если основная сессия разрывается, выбирается новая основная сессия в соответствии с параметрами, которые вы указываете при настройке подключения устройства CPE к оркестратору и контроллеру.

На рисунке ниже изображены сессии между тремя контроллерами и устройством CPE с двумя интерфейсами SD-WAN с типом WAN:

- 10.0.1.1 → ctl1:6653

- 10.0.2.1 → ctl1:6654
- 10.0.1.1 → ctl2:6653
- 10.0.2.1 → ctl2:6654
- 10.0.1.1 → ctl3:6653
- 10.0.2.1 → ctl3:6654



Сессии между устройством CPE и тремя контроллерами

Для отображения таблицы устройств CPE с информацией об управляющих сессиях вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN, к которому подключены устройства, и в открывшемся меню настройки контроллера перейти в раздел **Коммутаторы**. Информация об управляющих сессиях отображается в следующих столбцах таблицы:

- **Имя** – имя устройства CPE.
- **ID** – порядковый номер устройства CPE. Устройство с наименьшим порядковым номером первым подключилось к контроллеру.
- **Статус** – статус устройства CPE по отношению к контроллеру:
  - **Активный** – устройство можно использовать для передачи трафика.
  - **Неактивный** –устройство невозможно использовать для передачи трафика.
- **Подключение –** статус подключения устройства CPE к контроллеру:
  - **Подключен** – между устройством и контроллером установлена управляющая сессия.
  - **Отключен** – между устройством и контроллером не установлена управляющая сессия.
- **MAC** – MAC-адрес устройства CPE.
- **Интерфейс** – интерфейсы SD-WAN с типом WAN, с которых установлены управляющие сессии до контроллера.
- **Основная сессия** – интерфейс SD-WAN с типом WAN, с которого установлена основная управляющая сессия до контроллера.
- **IP** – IP-адрес интерфейса SD-WANс типом WAN, с которого установлена управляющая сессия до контроллера.

- **Создан** – дата и время регистрации устройства CPE.
- **Адрес** – адрес площадки устройства CPE.
- **Задержка (мс.)** – время задержки в миллисекундах для управляющей сессии между устройством CPE и контроллером.
- **Описание** – краткое описание устройства CPE.

Автоматическая регистрация устройств CPE (ZTP)

Вам нужно автоматически зарегистрировать новые устройства CPE с помощью веб-адреса с базовыми параметрами. Сценарий автоматической регистрации устройства состоит из следующих этапов:

1. **Перевод прошивки устройства CPE в стартовое состояние**

   Для автоматической регистрации прошивка устройства CPE должна находиться в стартовом состоянии. Для перевода прошивки в базовое состояние подключитесь к консоли устройства CPE по SSH и выполните следующую команду:

   ```
   firstboot && reboot
   ```

2. **Создание шаблона CPE**

   Создайте шаблон CPE. Вы можете использовать созданный шаблон CPE для настройки других устройств. Необязательный этап, если вы уже создали шаблон CPE.

3. **Добавление устройства CPE**

   Добавьте устройство CPE. При добавлении назначьте устройству CPE ранее созданный шаблон и выберите, должно ли устройство автоматически включиться после регистрации. Добавленное устройство CPE имеет статус *Ожидание*.

4. **Двухфакторная аутентификация**

   Если вы хотите безопасно зарегистрировать устройство CPE, используйте двухфакторную аутентификацию. Необязательный этап.

5. **Генерация веб-адреса с базовыми параметрами**

   Сгенерируйте веб-адрес с базовыми параметрами устройства CPE.

6. **Регистрация устройства CPE**

   Выполните следующие действия:

   1. Подключитесь к LAN-интерфейсу устройства CPE и получите IP-адрес по DHCP.
   2. Перейдите по веб-адресу с базовыми параметрами устройства CPE или откройте файл в формате HTML, который вы сохранили при генерации веб-адреса.
   3. На открывшейся странице нажмите на кнопку **Применить конфигурацию**.
   4. Дождитесь применения базовых параметров и перезагрузки устройства CPE.

   При успешном применении параметров устройство CPE подключится к оркестратору, будет сопоставлено с ранее добавленной записью в веб-интерфейсе и автоматически зарегистрируется. Зарегистрированное устройство имеет статус *Зарегистрировано* и находится в состоянии *Активировано* или *Деактивировано*.

7. **Включение устройства CPE**

   Если при добавлении устройства CPE вы указали, что оно не должно автоматически включиться, включите устройство. Включенное устройство CPE имеет статус *Зарегистрировано* и находится в состоянии *Активировано*. Необязательный этап.

Повторная регистрация устройств CPE

Если вы удаляете устройство CPE, на нем сохраняются базовые параметры. Такое устройство CPE можно повторно зарегистрировать без использования веб-адреса с базовыми параметрами.

> При повторной регистрации устройства CPE невозможно использовать двухфакторную аутентификацию. Если вы хотите использовать двухфакторную аутентификацию, проведите автоматическую регистрацию устройства CPE.

Сценарий повторной регистрации устройства CPE состоит из следующих этапов:

1. **Создание шаблона CPE**

   Создайте шаблон CPE. Вы можете использовать созданный шаблон CPE для настройки других устройств. Необязательный этап, если вы уже создали шаблон CPE.

2. **Подключение устройства CPE к оркестратору**

   Перезагрузите устройство CPE, чтобы оно подключилось к оркестратору. При успешном подключении устройство CPE отобразится в веб-интерфейсе оркестратора со статусом *Неизвестно*.

3. **Регистрация устройства CPE**

   Вручную зарегистрируйте устройство CPE. При регистрации назначьте устройству CPE ранее созданный шаблон и выберите, должно ли устройство автоматически включиться после регистрации. Зарегистрированное устройство имеет статус *Зарегистрировано* и находится в состоянии *Активировано* или *Деактивировано*.

4. **Включение устройства CPE**

   Если при ручной регистрации устройства CPE вы указали, что оно не должно автоматически включиться, включите устройство. Включенное устройство CPE имеет статус *Зарегистрировано* и находится в состоянии *Активировано*. Необязательный этап.

Работа с шаблонами CPE

Таблица шаблонов CPE отображается в разделе **SD-WAN → Шаблоны CPE**. Информация о шаблонах CPE отображается в следующих столбцах таблицы:

- **ID** – идентификатор шаблона CPE.
- **Имя** – имя шаблона CPE.
- **Использование** – используется ли шаблон 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 инструкции Работа с таблицами компонентов решения.

Параметры шаблона CPE отображаются на следующих вкладках:

- **Информация** – основная информация о шаблоне CPE. Вы можете изменить имя шаблона в поле **Имя**.
- **Мультипутевая передача** – параметры транспортных путей.
- **Деактивация** – параметры автоматического удаления и выключения устройства CPE.
- **Шифрование** – шифрование трафика.
- **Скрипты** – скрипты для дополнительной настройки устройства CPE.
- **Параметры SD-WAN** – на этой вкладке отображаются следующие вкладки:
  - **Глобальные настройки** – параметры подключения устройства CPE к оркестратору и контроллеру.
  - **Интерфейсы** – интерфейсы SD-WAN.
- **Топология** – топологические теги для построения туннелей между устройствами CPE.
- **Параметры сети** – сетевые интерфейсы.
- **Параметры BGP** – протокол BGP для обмена маршрутами между устройствами CPE и внешними сетевыми устройствами. На этой вкладке отображаются следующие вкладки:
  - **Общие параметры** – основные параметры протокола BGP.
  - **BGP-соседи** – BGP-соседи.
  - **Группы BGP-соседей** – группы BGP-соседей.
- **VRF** – виртуальные таблицы маршрутизации.
- **OSPF** – протокол OSPF для обмена маршрутами между устройствами CPE и внешними сетевыми устройствами. На этой вкладке отображаются следующие вкладки:
  - **Общие 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).

- **Параметры 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:
  - **Общие 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.
- **Мониторинг** – параметры мониторинга устройства CPE.
- **Транспортные сервисы** – транспортные сервисы.
- **Журналы** – параметры журналов.
- **NTP** – NTP-серверы для синхронизации времени.
- **VIM** – параметры VIM. Эта вкладка отображается, только если при создании шаблона 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. Значение по умолчанию.
   - **uCPE** – шаблон устройства uCPE. В состав устройств uCPE входит гипервизор, поэтому на нем можно развернуть виртуальные сетевые функции и VIM.

5. Нажмите на кнопку **Создать**.

Шаблон CPE будет создан и отобразится в таблице.

Экспорт шаблона CPE

Вы можете экспортировать шаблон CPE, чтобы затем импортировать его в другой шаблон. Когда вы экспортируете шаблон CPE, на ваше локальное устройство сохраняется архив 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.

Чтобы экспортировать 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 будет 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. В архиве не содержится информация об устройствах CPE, использующих шаблон.

Импорт шаблона CPE

Вы можете импортировать в шаблон CPE ранее экспортированный шаблон. Параметры шаблона CPE выстраиваются в соответствии с параметрами импортированного шаблона. При импорте можно выбрать вкладки, которые вы хотите оставить без изменений.

Шаблон CPE, в который был импортирован другой шаблон, остается примененным к устройствам, но параметры этих устройств не изменяются.

Чтобы импортировать шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, в который вы хотите импортировать другой шаблон.

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

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Импортировать**.

4. В открывшемся окне снимите флажки рядом с вкладками шаблона CPE, которые вы хотите оставить без изменения после импорта.

5. В поле **Файл** укажите путь к архиву в формате TAR.GZ.

6. Нажмите на кнопку **Импортировать**.

Параметры шаблона CPE будут изменены в соответствии с параметрами импортируемого шаблона.

Клонирование шаблона CPE

Вы можете клонировать шаблон CPE, чтобы создать такой же шаблон 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 будет 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**.

Копия шаблона CPE с новым именем будет создана 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 будет 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 будет 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

Вы можете просмотреть, какие устройства CPE используют шаблон. Если шаблон CPE используется хотя бы одним устройством, этот шаблон невозможно удалить.

Чтобы просмотреть использование шаблона CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE, использование которого вы хотите просмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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 **Устройства CPE**, в котором отображается таблица устройств CPE, использующих шаблон.

Удаление шаблона CPE

Вы не можете удалить шаблон CPE, если он используется хотя бы одним устройством. Вам нужно просмотреть использование шаблона CPE и убедиться, что он не используется ни одним устройством.

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 будет 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

Таблица устройств CPE отображается в разделе **SD-WAN → Устройства CPE**. Информация об устройствах CPE отображается в следующих столбцах таблицы:

- **DPID** – идентификатор DPID устройства CPE.
- **C/N** – серийный номер устройства CPE.
- **Модель** – модель устройства CPE.
- **Версия ПО** – версия прошивки устройства CPE. Устаревшие прошивки подсвечиваются оранжевым цветом.
- **Шаблон CPE** – шаблон CPE, используемый устройством.
- **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** – устройство CPE регистрируется.
  - **Ошибка** – при регистрации устройства CPE возникла ошибка.
  - **Зарегистрировано** – устройство CPE успешно зарегистрировано.
  - **Конфигурация** – на устройстве CPE запускаются скрипты.
- **Состояние** – состояние устройства CPE:

- **Активировано** – со стороны оркестратора к устройству CPE применен назначенный шаблон. Со стороны контроллера устройство CPE можно использовать для передачи трафика.
- **Деактивировано** (в статусе **Ожидание**) – со стороны оркестратора к устройству CPE не применен назначенный шаблон. Со стороны контроллера устройство CPE невозможно использовать для передачи трафика.
- **Деактивировано** (в статусе **Зарегистрировано**) – оркестратор не отвечает на REST API-запросы, поступающие от устройства CPE. Со стороны контроллера устройству CPE заблокирована передача трафика по туннелям.

- **Подключение** – подключено ли устройство CPE к контроллеру:
  - **Подключено**.
  - **Отключено**.
- **Топологические теги** – топологические теги, назначенные 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.
- **Использование** – используются ли интерфейсы SD-WAN устройства CPE транспортными сервисами:
  - **Да**.
  - **Нет**.
- **Транспортный тенант** – тенант, которому добавлено устройство CPE.
- **Клиентский тенант** – тенант организации клиента, которому добавлено устройство CPE.
- **Адрес** – адрес устройства CPE.
- **Управляющий IP** – IP-адрес, назначенный устройству CPE управляющей подсетью.
- **Контроллеры** – IP-адреса и номера портов контроллеров, 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.

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

Параметры устройства CPE отображаются на следующих вкладках:

- **Конфигурация** – основная информация об устройстве CPE. Вы можете указать краткое описание устройства CPE в поле **Описание** и просмотреть 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** – шифрование трафика.
- **Сервисные запросы** – сервисные запросы устройства CPE.
- **Теги** – теги для группировки устройств CPE.
- **Скрипты** – скрипты для дополнительной настройки устройства CPE.
- **Параметры SD-WAN** – на этой вкладке отображаются следующие вкладки:
  - **Глобальные настройки** – параметры подключения устройства CPE к оркестратору и контроллеру.
  - **Интерфейсы** – интерфейсы SD-WAN.
- **Топология** – топологические теги для построения туннелей между устройствами CPE.
- **Параметры сети** – сетевые интерфейсы.
- **Параметры межсетевого экрана** – параметры межсетевого экрана.
- **VRF** – виртуальные таблицы маршрутизации.
- **Параметры BGP** – протокол BGP для обмена маршрутами между устройствами CPE и внешними сетевыми устройствами. На этой вкладке отображаются следующие вкладки:
  - **Общие параметры** – основные параметры протокола BGP.
  - **BGP-соседи** – BGP-соседи.
  - **Группы BGP-соседей** – группы BGP-соседей.
- **OSPF** – протокол OSPF для обмена маршрутами между устройствами CPE и внешними сетевыми устройствами. На этой вкладке отображаются следующие вкладки:
  - **Общие 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).
- **Параметры 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:
    - **Общие 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.
- **UNI** – UNI на устройстве CPE.
- **Модемы** – параметры модемов устройства CPE.
- **Туннели** – параметры туннелей.
- **Мультипутевая передача** – параметры транспортных путей.
- **Активация** – параметры двухфакторной аутентификации устройства CPE.
- **Деактивация** – параметры автоматического удаления и выключения устройства CPE.
- **Журналы** – 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 устройства 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 подключенным устройством. Вы можете добавить устройство CPE текущему экземпляру SD-WAN, тенанту или другому экземпляру SD-WAN.

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 → Устройства 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 ранее созданного тенанта и в блоке **Устройства CPE** нажмите на кнопку **+ Устройство CPE**.

   - Если вы хотите добавить устройство CPE другому экземпляру SD-WAN, в меню перейдите в подраздел **SD-WAN → Экземпляры SD-WAN**, нажмите на ранее развернутый экземпляр 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.

4. В раскрывающемся списке **Состояние** выберите состояние устройства после регистрации:

   - **Активировано** – применить к устройству шаблон CPE и использовать для передачи трафика. Значение по умолчанию.

   - **Деактивировано** – не применять к устройству шаблон CPE.

5. При необходимости в поле **Описание** введите краткое описание устройства.

6. Если вы добавляете устройство CPE экземпляру SD-WAN, раскрывающемся списке **Тенант** выберите тенанта, которому вы хотите назначить устройство. Вы можете выбрать пул экземпляров SD-WAN или отдельный экземпляр из пула.

7. При необходимости в раскрывающемся списке **Клиентский тенант** выберите тенанта организации вашего клиента.

8. Если вы хотите создать UNI на устройстве CPE с помощью шаблона UNI, в раскрывающемся списке **Шаблон UNI** выберите ранее созданный шаблон UNI.

9. В раскрывающемся списке **Шаблон CPE** выберите ранее созданный шаблон CPE, в соответствии с которым вы хотите настроить устройство CPE.

10. В раскрывающемся списке **Шаблон NetFlow** выберите ранее созданный шаблон NetFlow, в соответствии с которым вы хотите настроить основные параметры NetFlow на устройстве CPE.

11. В раскрывающемся списке **Шаблон межсетевого экрана** выберите ранее 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 перейдет в статус *Ожидание*, и вы получите один из следующих результатов:

- Если вы добавили устройство CPE текущему экземпляру SD-WAN, устройство отобразится в таблице.

- Если вы добавили устройство CPE тенанту, устройство отобразится в блоке **Устройства CPE**.

- Если вы добавили устройство CPE другому экземпляру SD-WAN, веб-интерфейс оркестратора экземпляра откроется в новой вкладке браузера, вы автоматически войдете в него и перейдете в подраздел **Устройства CPE**. Устройство CPE отобразится в таблице.

Генерация веб-адреса с базовыми параметрами устройства CPE

Вам нужно сгенерировать веб-адрес с базовыми параметрами устройства CPE, если вы проводите автоматическую регистрацию устройства. Вы можете указать шаблон генерируемого веб-адреса при настройке подключения устройства CPE к оркестратору и контроллеру. Сгенерированный веб-адрес содержит следующую информацию:

- 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.

Максимальный размер веб-адреса с базовыми параметрами устройства CPE не должен превышать 64 килобайта.

Чтобы сгенерировать веб-адрес с базовыми параметрами устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, для которого вы хотите сгенерировать веб-адрес с базовыми параметрами.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Получить URL активации**.

   Откроется окно с веб-адресом с базовыми параметрами устройства CPE.

4. 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 **Сохранить в HTML**.

   Вам нужно перейти по веб-адресу или открыть файл в формате HTML на устройстве CPE, которое вы хотите автоматически зарегистрировать.

5. Если вы хотите установить сертификаты на устройстве CPE с версией прошивки 23.07, выполните следующие действия:

a. В раскрывающемся списке **Версия** выберите **23.07**.

b. Нажмите на кнопку **Копировать** рядом со всеми сгенерированными веб-адресами.

c. Сохраните скопированные веб-адреса.

Вам нужно поочередно перейти по скопированным веб-адресам на устройстве CPE, на котором вы хотите установить сертификаты.

Ручная регистрация устройства CPE

Вам нужно вручную зарегистрировать устройство CPE в веб-интерфейсе при повторной регистрации устройства. При регистрации не требуется подключаться к облачным сервисам "Лаборатории Касперского".

Чтобы вручную зарегистрировать устройство CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, которое вы хотите зарегистрировать вручную.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 после регистрации:

   - **Активировано** – применить к устройству шаблон CPE и использовать для передачи трафика. Значение по умолчанию.
   - **Деактивировано** – не применять к устройству шаблон CPE.

5. При необходимости в поле **Описание** введите краткое описание устройства.

6. В раскрывающемся списке **Тенант** выберите ранее созданного тенанта, которому вы хотите назначить устройство. Вы можете выбрать пул экземпляров SD-WAN или отдельный экземпляр из пула.

7. При необходимости в раскрывающемся списке **Клиентский тенант** выберите тенанта организации вашего клиента.

8. Если вы хотите создать UNI на устройстве CPE с помощью шаблона UNI, в раскрывающемся списке **Шаблон UNI** выберите ранее созданный шаблон UNI.

9. В раскрывающемся списке **Шаблон CPE** выберите ранее созданный шаблон CPE, в соответствии с которым вы хотите настроить устройство CPE.

10. В раскрывающемся списке **Шаблон NetFlow** выберите ранее созданный шаблон NetFlow, в соответствии с которым вы хотите настроить основные параметры NetFlow на устройстве CPE.

11. В раскрывающемся списке **Шаблон межсетевого экрана** выберите ранее 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 → Устройства CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, регистрацию которого вы хотите отменить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 изменится на *Ожидание*.

Указание адреса устройства CPE

Чтобы указать адрес устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, адрес которого вы хотите указать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 предлагается 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. Выключенные устройства CPE невозможно использовать для передачи трафика.

Чтобы включить или выключить устройство CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, которое вы хотите включить или выключить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Активировать** или **Деактивировать**.

Устройство CPE будет включено или выключено.

Перезагрузка устройства CPE

Чтобы перезагрузить устройство CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, которое вы хотите перезагрузить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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

При выключении питания устройства CPE в его оперативную систему отправляется команда `shutdown`.

Чтобы выключить питание устройства CPE:

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

Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, питание которого вы хотите выключить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Выключить**.

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

Питание устройства CPE будет выключено.

Подключение к консоли устройства CPE

Чтобы подключиться к консоли устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, к консоли которого вы хотите подключиться.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 просмотреть пароль устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, пароль которого вы хотите просмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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, и интерфейсы SD-WAN из устройства CPE:

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

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 ваше локальное устройство сохранится 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 → Устройства CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство 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 будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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.

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 → Устройства 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.

В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 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 двухфакторной аутентификации в базу данных оркестратора записывается токен (ключ безопасности), который затем вы помещаете на устройство CPE с помощью веб-адреса с базовыми параметрами. Регистрация проходит успешно, если при подключении устройства CPE к оркестратору помещенный на устройство токен совпадает с токеном в базе данных оркестратора.

Чтобы использовать двухфакторную аутентификацию устройства CPE:

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

Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, для которого вы хотите использовать двухфакторную аутентификацию.

В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Активация**.

Отобразятся параметры двухфакторной аутентификации.

4. В раскрывающемся списке **Двухфакторная аутентификация** выберите **Включено**. По умолчанию выбрано значение **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.

Таблица сертификатов отображается 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 инструкции 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 ранее 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.

Краткий 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 и при этом выполните следующие действия:

   1. В раскрывающемся списке **Версия** выберите **23.07**.
   2. Нажмите на кнопку **Копировать** рядом со всеми сгенерированными веб-адресами.
   3. Сохраните скопированные веб-адреса.

3. **Установка сертификатов на устройстве CPE**

   Поочередно перейдите по скопированным веб-адресам на устройстве CPE, на котором вы хотите установить сертификаты.

Устройство CPE будет перезагружаться после установки каждого 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.

      В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки 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.

Автоматическое удаление и выключение устройств CPE

Вы можете указать в шаблоне CPE или на устройстве время, по прошествии которого устройство должно быть удалено или выключено (англ. disabled) 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.

Когда вы указываете время автоматического удаления или выключения в шаблоне CPE, это время автоматически используется для всех использующих шаблон устройств.

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 и в отобразившейся области настройки выберите вкладку **Деактивация**.

   - Если вы хотите настроить автоматическое удаление и выключение на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Деактивация** и установите флажки **Переопределить**.

   Отобразятся параметры автоматического удаления и выключения устройства CPE.

2. Включите автоматическое удаление устройства CPE, выполнив следующие действия:

   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 должно быть удалено 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, выполнив следующие действия:

   a. Установите флажок **Включить** рядом с полем **Время деактивации (сек.)**.

   b. В поле **Время деактивации (сек.)** введите время в секундах, по прошествии которого устройство CPE должно быть выключено 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

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, к которому оно относится.

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 → Устройства 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.

      В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 → Добавить 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 → Устройства 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.

      В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 можно 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. Когда вы указываете параметры журналов в шаблоне CPE, эти параметры автоматически распространяются на все использующие шаблон устройства.

Чтобы настроить журналы на устройствах CPE:

1. 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 и в отобразившейся области настройки выберите вкладку **Журналы**.
   - Если вы хотите настроить журналы на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Журналы** и установите флажок **Переопределить**.

   Отобразятся параметры журналов.

2. В поле **Размер файлов журнала (КБ)** введите размер журналов на устройстве CPE в килобайтах. Диапазон значений: от 64 до 2048. По умолчанию указано значение 64. Если максимальный размер журналов превышается, новые журналы перезаписывают наиболее старые журналы.

3. Если вы хотите, чтобы устройство CPE отправляло журналы на внешний Syslog-сервер, укажите Syslog-сервер, выполнив следующие действия:

   a. В поле **IP или FQDN Syslog-сервера** введите IP-адрес Syslog-сервера.

   b. В поле **Порт Syslog-сервера** введите номер порта Syslog-сервера. Диапазон значений: от 0 до 65 353.

   c. В раскрывающемся списке **Протокол Syslog-сервера** выберите протокол передачи журналов на Syslog-сервер:

- **UDP** – значение по умолчанию.
- **TCP**.

d. В поле **Префикс для журналов** введите префикс, который устройство CPE должно назначать журналам. Максимальная длина: 256 символов.

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

Указание NTP-серверов на устройствах CPE

Вам нужно указать внутренний или внешний NTP-сервер, или пул серверов для устройств CPE, чтобы на этих устройствах отображалось точное время. При необходимости точно отображать время на сетевых устройствах, которые подключены к устройству CPE, это устройство можно использовать как NTP-сервер.

Вы можете указать NTP-сервер в шаблоне CPE или на устройстве. Когда вы указываете NTP-сервер в шаблоне CPE, этот сервер автоматически указывается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **NTP**.
   - Если вы хотите указать NTP-сервер на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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**. По умолчанию флажок установлен.

3. Если вы хотите использовать устройство CPE как NTP-сервер, установите флажок **Использовать как NTP-сервер**. По умолчанию флажок снят.

4. Укажите NTP-сервер или пул серверов, выполнив следующие действия:

   a. В блоке **NTP-серверы** нажмите на кнопку **+ Добавить**.

   b. В отобразившемся поле введите IP-адрес или FQDN NTP-сервера или 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 сервер, нажав рядом с ним на значок удаления ✕.

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

Вы можете просмотреть параметры синхронизации времени на устройстве CPE, запросив диагностическую информацию.

Работа с модемами

Устройство CPE может иметь до четырех модемов для подключения к сети оператора связи. Для отображения таблицы модемов вам нужно перейти в раздел **SD-WAN → Устройства 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.
- **DNS1**, **DNS2** – 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** – используется ли на модеме роуминг:
  - **Да**.
  - **Нет**.
- **Проверка HTTP** – результат проверки модемом доступности интернета с помощью HTTP.

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

Работа с прошивками

Новые версии программного обеспечения устройств CPE распространяются специалистами "Лаборатории Касперского" в виде прошивок (англ. firmware). Вы получаете архив в формате TAR.GZ, содержащий прошивку и файлы с ее параметрами в формате YAML. Прошивку необходимо загрузить в веб-интерфейс оркестратора и обновить на устройствах.

Устаревшие прошивки подсвечиваются оранжевым цветом в столбце **Версия ПО** таблицы устройств CPE. Устаревшие прошивки также можно найти с помощью фильтра **Необходимо обновление**, который отображается в верхней части таблицы.

Вы можете обновить прошивку на выбранных вручную устройствах CPE или на устройствах с указанными тегами. Если вы обновляете прошивку на выбранных вручную устройствах CPE, автоматически создается задача по обновлению в планировщике задач. Если вы обновляете прошивку на устройствах CPE с указанными тегами, вам нужно вручную создать задачу по обновлению в планировщике задач. В процессе обновления прошивки устройство CPE перезагружается.

Таблица прошивок отображается 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 которыми совместима прошивка.

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

Загрузка прошивки в веб-интерфейс оркестратора

Чтобы загрузить прошивку в веб-интерфейс оркестратора:

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

   Отобразится таблица прошивок.

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

3. Укажите путь к архиву с прошивкой. При указании пути вы можете выбрать несколько архивов одновременно.

Прошивка будет загружена и отобразится в таблице.

Обновление прошивки на выбранных вручную устройствах CPE

Чтобы обновить прошивку на выбранных вручную устройствах CPE:

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

Отобразится таблица устройств CPE.

2. Установите флажки рядом с устройствами CPE, на которых вы хотите обновить прошивку.
3. В верхней части таблицы нажмите на кнопку **Действия** → **Обновить прошивку**.
4. В открывшемся окне в поле **Имя** введите имя запланированной задачи.
5. В раскрывающемся списке **Версия** выберите ранее загруженную прошивку.
6. В поле **Дата и время выполнения** введите дату и время выполнения запланированной задачи. По умолчанию указана дата и время в момент, когда вы начали создавать запланированную задачу.
7. Если вы хотите сбросить параметры устройства CPE до заводских значений после обновления прошивки, снимите флажок **Сохранить конфигурацию**. Когда флажок установлен, после обновления прошивки параметры устройства CPE остаются без изменений. По умолчанию флажок установлен.

   При сбросе параметров до заводских значений устройство CPE отключается от оркестратора. Для повторного подключения устройства CPE к оркестратору вам нужно провести его автоматическую регистрацию (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**. По умолчанию флажок снят.
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 отображается в следующих столбцах:

   - **DPID** – идентификатор DPID устройства CPE.
   - **Модель** – модель устройства CPE.
   - **Имя** – имя устройства CPE.
   - **Версия ПО** – версия прошивки устройства CPE.
   - **Транспортный тенант** – тенант, которому добавлено устройство CPE.
   - **Причина** – причина, по которой прошивку невозможно обновить. Этот столбец отображается только в нижней таблице.

   Если в нижнюю таблицу попали устройства CPE, на которых вы не хотите обновлять прошивку, вы можете перенести эти устройства в верхнюю таблицу.

10. Нажмите на кнопку **Запланировать**.

Запланированная задача по обновлению прошивки будет создана и отобразится в таблице в разделе **Планировщик**. Обновление прошивки на устройстве CPE начнется в указанное время.

Обновление прошивки на устройствах CPE с указанными тегами

Чтобы обновить прошивку на устройствах CPE с указанными тегами:

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

   Отобразится таблица запланированных задач.

2. В верхней части страницы нажмите на кнопку **+ Отложенная задача**.

3. В открывшемся окне в раскрывающемся списке **Тип** выберите **Отложенное обновление прошивки**.

4. В поле **Имя** введите имя запланированной задачи.

5. В раскрывающемся списке **Версия** выберите ранее загруженную прошивку.

6. В поле **Дата и время выполнения** введите дату и время выполнения запланированной задачи. По умолчанию указана дата и время в момент, когда вы начали создавать запланированную задачу.

7. Если вы хотите сбросить параметры устройства CPE до заводских значений после обновления прошивки, снимите флажок **Сохранить конфигурацию**. Когда флажок установлен, после обновления прошивки параметры устройства CPE остаются без изменений. По умолчанию флажок установлен.

   При сбросе параметров до заводских значений устройство CPE отключается от оркестратора. Для повторного подключения устройства CPE к оркестратору вам нужно провести его автоматическую регистрацию (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**. По умолчанию флажок снят.

9. В поле **Теги** введите теги устройств CPE, на которых вы хотите обновить прошивку.

10. 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 отображается в следующих столбцах:

    - **DPID** – идентификатор DPID устройства CPE.
    - **Модель** – модель устройства CPE.
    - **Имя** – имя устройства CPE.
    - **Версия ПО** – версия прошивки устройства CPE.
    - **Транспортный тенант** – тенант, которому добавлено устройство CPE.
    - **Причина** – причина, по которой прошивку невозможно обновить. Этот столбец отображается только в нижней таблице.

    Если в нижнюю таблицу попали устройства CPE, на которых вы не хотите обновлять прошивку, вы можете перенести эти устройства в верхнюю таблицу.

11. Нажмите на кнопку **Создать**.

Запланированная задача по обновлению прошивки будет создана и отобразится в таблице. Обновление прошивки на устройстве CPE начнется в указанное время.

Удаление прошивки

Вы не можете удалить прошивку, которая используется в запланированной задаче.

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**.

   Прошивка будет удалена и перестанет отображаться в таблице.

Дополнительная настройка устройств CPE с помощью скриптов

Для дополнительной настройки устройств CPE используются скрипты. Вам нужно добавить скрипт в шаблон CPE, чтобы этот скрипт автоматических добавился на всех использующих шаблон устройствах. 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 пользователя, от имени которого VNFM должен запускать скрипты. При необходимости вы можете изменить номер порта и имя пользователя.

Таблица скриптов отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы скриптов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Скрипты**.
- Для отображения таблицы скриптов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Скрипты**.

Информация о скриптах отображается в следующих столбцах таблицы:

- **Имя** – имя скрипта.
- **Исполнитель скрипта** – интерпретатор.
- **Аутентификация** – тип аутентификации VNFM в устройстве CPE.

- **Пользовательский интерпретатор** – путь к пользовательскому интерпретатору.
- **Время (сек.)** – время в секундах, по прошествии которого VNFM должен перестать предпринимать попытки запуска скрипта, который не запустился с первого раза.
- **Повторный запуск** – должен ли скрипт быть повторно запущен:
  - **Да**.
  - **Нет**.
- **Стадия** – стадия работы устройства CPE, на которой VNFM должен запускать 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

Вы можете добавить скрипт в шаблон CPE. Когда вы добавляете скрипт в шаблон CPE, этот скрипт автоматически добавляется на всех использующих шаблон устройствах.

Чтобы добавить скрипт:

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 будет выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, учетные данные пользователя 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: 255 символов.

6. В поле **Время (сек.)** введите время в секундах, по прошествии которого VNFM должен перестать предпринимать попытки запуска скрипта, который не запустился с первого раза. По умолчанию указано значение `360`.

7. В раскрывающемся списке **Исполнитель скрипта** выберите одно из следующих значений:
   - **Ansible –** значение по умолчанию.
   - **Shell**.
   - **Expect**.

- **Пользовательский** – использовать интерпретатор на устройстве CPE. При выборе этого значения в поле **Пользовательский интерпретатор** введите путь к интерпретатору.

8. В раскрывающемся списке **Стадия** выберите, на какой стадии работы устройства CPE VNFM должен запускать скрипт:

   - **Регистрация** – значение по умолчанию.
   - **Удаление**.
   - **Вручную** – запускать скрипт только вручную.

9. При необходимости повторно запускать скрипт установите флажок **Повторный запуск**. По умолчанию флажок снят. 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.

Ручной запуск скриптов

Вы можете вручную запустить отдельный скрипт или все скрипты в шаблоне CPE или на устройстве. Когда вы запускаете скрипты в шаблоне CPE, эти скрипты автоматически запускаются на всех использующих шаблон устройствах или на устройствах с указанными тегами.

Ручной запуск скриптов 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 запустить скрипты.

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

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, учетные данные пользователя для запуска скриптов и таблица скриптов, если добавлен хотя бы один скрипт.

4. Если вы хотите запустить отдельный скрипт, выполните следующие действия:

   a. Нажмите на кнопку **Запустить** рядом со скриптом, который вы хотите запустить.

   b. В открывшемся окне выберите, на каких устройствах CPE должен быть запущен скрипт:

   - **Запустить скрипт <имя скрипта> на всех связанных CPE** – запустить скрипт на всех использующих шаблон CPE устройствах. Значение по умолчанию.
   - **Запустить скрипт <имя скрипта> на всех связанных CPE с тегами** – запустить скрипт на использующих шаблон CPE устройствах с указанными тегами. При выборе этого значения в нижней части окна укажите теги.

5. Если вы хотите 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 должны быть запущены скрипты:

   - **Запустить скрипты на всех связанных CPE** – запустить скрипты на всех использующих шаблон CPE устройствах. Значение по умолчанию.
   - **Запустить скрипты на всех связанных CPE с тегами** – запустить скрипты на использующих шаблон CPE устройствах с указанными тегами. При выборе этого значения в нижней части окна укажите теги.

6. Нажмите на кнопку **Запустить**.

Скрипты будут запущены.

Ручной запуск скриптов на устройстве CPE

Чтобы вручную запустить скрипты на устройстве CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, в котором вы хотите запустить скрипты.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, учетные данные пользователя для запуска скриптов и таблица скриптов, если добавлен хотя бы один скрипт.

4. Выполните одно из следующих действий:

   - Если вы хотите запустить отдельный скрипт, нажмите на кнопку **Запустить** рядом с этим скриптом.

- Если вы хотите 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

Запланированные задачи по запуску скриптов на устройствах CPE можно создать в планировщике задач. При создании запланированной задачи необходимо выбрать шаблон CPE, скрипты, а также устройства, на которых скрипты должны быть запущены.

Вы можете запустить скрипты на всех использующих шаблон CPE устройствах или ограничить их количество, указав теги или выбрав устройства вручную.

Чтобы создать запланированную задачу по запуску скриптов:

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

   Отобразится таблица запланированных задач.

2. В верхней части страницы нажмите на кнопку **+ Отложенная задача**.

3. В открывшемся окне в раскрывающемся списке **Тип** выберите **Запуск скрипта**.

4. В поле **Имя** введите имя запланированной задачи.

5. В раскрывающемся списке **CPE для запуска скрипта** выберите, на каких устройствах CPE скрипты должны быть запущены:

   - **Все CPE с выбранным шаблоном** – запустить скрипты на всех использующих шаблон CPE устройствах.
   - **Все CPE с выбранным шаблоном и определенными тегами** – запустить скрипты на использующих шаблон CPE устройствах с указанными тегами. При выборе этого значения в поле **Теги** укажите теги устройств CPE.
   - **Определенные CPE с выбранным шаблоном** – запустить скрипты на использующих шаблон CPE устройствах, выбранных вручную. При выборе этого значения в блоке **CPE** 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 **Дата и время выполнения** введите дату и время выполнения запланированной задачи. По умолчанию указаны дата и время в момент, когда вы начали создавать запланированную задачу.

9. Нажмите на кнопку **Создать**.

Запланированная задача по запуску скрипта будет создана и отобразится в таблице.

Изменение скрипта

Вы можете изменить скрипт только в шаблоне CPE. Когда вы изменяете скрипт в шаблоне CPE, этот скрипт автоматически изменяется на всех использующих шаблон устройствах.

Чтобы изменить скрипт:

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 будет выбрана вкладка **Информация**, на которой отображается основная информация о шаблоне CPE.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, учетные данные пользователя 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 в поле **Имя** введите имя скрипта. Максимальная длина: 255 символов.

6. В поле **Время (сек.)** введите время в секундах, по прошествии которого VNFM должен перестать предпринимать попытки запуска скрипта, который не запустился с первого раза. По умолчанию указано значение `360`.

7. В раскрывающемся списке **Исполнитель скрипта** выберите одно из следующих значений:

   - **Ansible –** значение по умолчанию.
   - **Shell**.
   - **Expect**.
   - **Пользовательский** – использовать интерпретатор на устройстве CPE. При выборе этого значения в поле **Пользовательский интерпретатор** введите путь к интерпретатору.

8. В раскрывающемся списке **Стадия** выберите, на какой стадии работы устройства CPE VNFM должен запускать скрипт:

   - **Регистрация** – значение по умолчанию.
   - **Удаление**.
   - **Вручную** – запускать скрипт только вручную.

9. При необходимости повторно запускать скрипт установите флажок **Повторный запуск**. По умолчанию флажок снят. 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 изменен и обновится в таблице.

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

Удаление скрипта

Вы можете удалить скрипт только в шаблоне CPE. Когда вы удаляете скрипт в шаблоне CPE, этот скрипт автоматически удаляется на всех использующих шаблон устройствах.

Удаленные скрипты невозможно восстановить.

Чтобы удалить скрипт:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на 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.

3. Выберите вкладку **Скрипты**.

   Отобразится номер порта для подключения VNFM к устройству CPE, учетные данные пользователя 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.

Работа с сетевыми интерфейсами

Сетевые интерфейсы соответствуют физическим 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.

Таблица сетевых интерфейсов отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы сетевых интерфейсов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Параметры сети**.

- Для отображения таблицы сетевых интерфейсов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Параметры сети**.

Информация о сетевых интерфейсах отображается в следующих столбцах таблицы:

- **Псевдоним** – имя сетевого интерфейса для построения соответствия между сетевым интерфейсом и OpenFlow-портом. Вам нужно указать это имя при создании интерфейса SD-WAN с типом WAN.

- **Унаследовано** – унаследован ли сетевой интерфейс из шаблона CPE:

  - **Да**.

  - **Нет**.

  Этот столбец отображается только на устройстве CPE.

- **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.

- **Включать автоматически** – должен ли сетевой интерфейс автоматически включаться при включении устройства CPE:

  - **Да**.

  - **Нет**.

Создание сетевых интерфейсов

Вы можете создать сетевой интерфейс в шаблоне CPE или на устройстве. Когда вы создаете сетевой интерфейс в шаблоне CPE, этот интерфейс автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.

   - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**.

   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 этот псевдоним при создании интерфейса SD-WAN с типом WAN. Максимальная длина: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите ранее созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина: 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. Если вы хотите создать мост из физических или виртуальных интерфейсов, имена которых указаны в поле **Имя интерфейса**, выполните следующие действия:

   a. Установите флажок **Мост**. По умолчанию флажок снят.

   b. Если вы хотите использовать на мосту протокол STP для предотвращения петель маршрутизации, установите флажок **STP**. По умолчанию флажок снят.

   c. В поле **Возраст (сек.)** введите время в секундах, в течение которого динамические записи должны храниться 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**. По умолчанию флажок снят.

8. В раскрывающемся списке **Протокол** выберите **DHCP-клиент**.

9. Если вы не хотите, чтобы сетевой интерфейс автоматически включался одновременно с устройством CPE, снимите флажок **Включать автоматически**. По умолчанию флажок установлен.

10. Если вы хотите, чтобы сетевому интерфейсу автоматически назначался IP-адрес, маршрут и шлюз по умолчанию, установите флажок **Назначать IP, маршрут и шлюз**. По умолчанию флажок снят.

11. Если вы не хотите, чтобы на сетевом интерфейсе по умолчанию использовался маршрут, полученный по протоколу DHCP, снимите флажок **Использовать маршрут по умолчанию**. По умолчанию флажок установлен.

12. При необходимости укажите DNS-сервер для сетевого интерфейса, выполнив следующие действия:

    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 сервер, нажав рядом с ним на значок удаления ✕.

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. Если вы создаете первый сетевой интерфейс, на который будет ссылаться интерфейс SD-WAN с типом WAN, в поле **Метрика маршрута** введите `100`. Для каждого следующего сетевого интерфейса, на который будет ссылаться интерфейс SD-WAN с типом WAN, требуется увеличить значение на 1. Например, для второго сетевого интерфейса введите `101`.

16. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

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

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.

   - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**.

   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 этот псевдоним при создании интерфейса SD-WAN с типом WAN. Максимальная длина: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите ранее созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина: 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. Если вы хотите создать мост из физических или виртуальных интерфейсов, имена которых указаны в поле **Имя интерфейса**, выполните следующие действия:

   a. Установите флажок **Мост**. По умолчанию флажок снят.

   b. Если вы хотите использовать на мосту протокол STP для предотвращения петель маршрутизации, установите флажок **STP**. По умолчанию флажок снят.

   c. В поле **Возраст (сек.)** введите время в секундах, в течение которого динамические записи должны храниться 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**. По умолчанию флажок снят.

8. В раскрывающемся списке **Протокол** выберите **Статический IPv4-адрес**.

9. Если вы не хотите, чтобы сетевой интерфейс автоматически включался одновременно с устройством CPE, снимите флажок **Включать автоматически**. По умолчанию флажок установлен.

10. Если вы хотите, чтобы сетевому интерфейсу автоматически назначался IP-адрес, маршрут и шлюз по умолчанию, установите флажок **Назначать IP, маршрут и шлюз**. По умолчанию флажок снят.

11. 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.

    - **Из пула IP-адресов** – назначить IPv4-адрес из указанного диапазона IP-адресов. При выборе этого значения в раскрывающемся списке **Пул IP** выберите ранее созданный диапазон IP-адресов.

    - **Из пула подсетей** – назначить IPv4-адрес из указанного диапазона подсетей. При выборе этого значения в раскрывающемся списке **Пул подсетей** выберите ранее созданный диапазон подсетей.

12. В поле **IPv4-шлюз** введите IPv4-адрес шлюза по умолчанию.

13. В поле **IPv4-трансляция** введите широковещательный адрес сетевого интерфейса. Если вы не указываете значение для этого параметра, оно генерируется автоматически.

14. При необходимости укажите DNS-сервер для сетевого интерфейса, выполнив следующие действия:

    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 сервер, нажав рядом с ним на значок удаления ✕.

15. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет фактический MAC-адрес сетевого интерфейса.

16. В поле **Переопределить MTU** введите значение MTU для сетевого интерфейса. Введенное значение заменяет MTU по умолчанию.

17. Если вы создаете первый сетевой интерфейс, на который ссылается интерфейс SD-WAN с типом WAN, в поле **Метрика маршрута** введите `100`. Для каждого следующего сетевого интерфейса, на который будет ссылаться интерфейс SD-WAN с типом WAN, требуется увеличить значение на 1. Например, для второго сетевого интерфейса введите `101`.

18. В блоке **DHCP-сервер** в раскрывающемся списке **Тип** выберите режим работы DHCP-сервера для сетевого интерфейса:

    - **Выключен** – значение по умолчанию.
    - **Ретранслятор**. При выборе этого значения в поле **IP DHCP-сервера** введите IP-адрес DHCP-сервера.
    - **Сервер**.

19. Если в раскрывающемся списке **Тип** вы выбрали **Сервер**, укажите параметры DHCP-сервера, выполнив следующие действия:

    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. По умолчанию указано значение `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. По умолчанию указано значение `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`. По умолчанию указано значение `12h`.

    d. При необходимости укажите DHCP-опцию, выполнив следующие действия:

        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 опцию, нажав рядом с ней на значок удаления ✕.

20. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

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

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.
   - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**.

   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 этот псевдоним при создании интерфейса SD-WAN с типом WAN. Максимальная длина: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите ранее созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина: 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. Если вы хотите создать мост из физических или виртуальных интерфейсов, имена которых указаны в поле **Имя интерфейса**, выполните следующие действия:

   a. Установите флажок **Мост**. По умолчанию флажок снят.

   b. Если вы хотите использовать на мосту протокол STP для предотвращения петель маршрутизации, установите флажок **STP**. По умолчанию флажок снят.

   c. В поле **Возраст (сек.)** введите время в секундах, в течение которого динамические записи должны храниться 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**. По умолчанию флажок снят.

8. В раскрывающемся списке **Протокол** выберите **Статический IPv6-адрес**.

9. Если вы не хотите, чтобы сетевой интерфейс автоматически включался одновременно с устройством CPE, снимите флажок **Включать автоматически**. По умолчанию флажок установлен.

10. Если вы хотите, чтобы сетевому интерфейсу автоматически назначался IP-адрес, маршрут и шлюз по умолчанию, установите флажок **Назначать IP, маршрут и шлюз**. По умолчанию флажок снят.

11. В поле **IPv6-адрес** введите IPv6-адрес сетевого интерфейса. Вы можете ввести несколько адресов через пробел.

12. В поле **IPv6-суффикс** введите IPv6-суффикс сетевого интерфейса. Максимальная длина: 30 символов.

13. В поле **IPv6-шлюз** введите IPv6-адрес шлюза по умолчанию.

14. В поле **Длина префикса** введите длину IPv6-префикса сетевого интерфейса. Диапазон значений: 12 до 127.

15. В поле **Суб-префикс DHCPv6** введите размер суб-префикса DHCPv6 сетевого интерфейса. Максимальная длина: 256 символов.

16. В поле **IPv6-префикс** введите IPv6-префикс сетевого интерфейса. Максимальная длина: 30 символов.

17. 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 класс, нажав рядом с ним на значок удаления ×.

18. При необходимости укажите DNS-сервер для сетевого интерфейса, выполнив следующие действия:

    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 сервер, нажав рядом с ним на значок удаления ×.

19. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет фактический MAC-адрес сетевого интерфейса.

20. В поле **Переопределить MTU** введите значение MTU для сетевого интерфейса. Введенное значение заменяет MTU по умолчанию.

21. Если вы создаете первый сетевой интерфейс, на который будет ссылаться интерфейс SD-WAN с типом WAN, в поле **Метрика маршрута** введите `100`. Для каждого следующего сетевого интерфейса, на который будет ссылаться интерфейс SD-WAN с типом WAN, требуется увеличить значение на 1. Например, для второго сетевого интерфейса введите `101`.

22. В блоке **DHCP-сервер** в раскрывающемся списке **Тип** выберите режим работы DHCP-сервера для сетевого интерфейса:

    - **Выключен** – значение по умолчанию.
    - **Ретранслятор**. При выборе этого значения в поле **IP DHCP-сервера** введите IP-адрес DHCP-сервера.
    - **Сервер**.

23. Если в раскрывающемся списке **Тип** вы выбрали **Сервер**, укажите параметры DHCP-сервера, выполнив следующие действия:

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. По умолчанию указано значение `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. По умолчанию указано значение `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`. По умолчанию указано значение `12h`.

d. При необходимости укажите DHCP-опцию, выполнив следующие действия:

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 опцию, нажав рядом с ней на значок удаления ×.

24. Нажмите на кнопку **Создать**.

Сетевой интерфейс будет создан и отобразится в таблице.

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

Создание сетевого интерфейса для подключения к LTE-сети

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.

- Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**.

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 и логическим WAN-интерфейсом. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

4. В раскрывающемся списке **Зона** выберите ранее созданную зону межсетевого экрана, в которую вы хотите добавить сетевой интерфейс.

5. В раскрывающемся списке **Протокол** выберите **QMI**.

6. В поле **Имя QMI** введите путь к модему на устройстве CPE. Максимальная длина: 30 символов. Например, вы можете ввести `/dev/cdc-wdm0`.

7. В поле **APN** введите идентификатор APN оператора связи, выпустившего SIM-карту, установленную в модеме. Максимальная длина: 30 символов.

8. 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.

9. В поле **Имя пользователя для аутентификации PAP/CHAP** введите имя пользователя для PAP/CHAP-аутентификации. Максимальная длина: 30 символов. Если вы не хотите использовать аутентификацию, не указывайте значение для этого параметра.

10. В поле **Пароль для аутентификации PAP/CHAP** введите пароль для PAP/CHAP-аутентификации. Максимальная длина: 30 символов. Если вы не хотите использовать аутентификацию, не указывайте значение для этого параметра.

11. В поле **PIN-код** введите PIN-код SIM-карты, установленной в модеме. Максимальная длина: 4 цифры.

12. В поле **Задержка** введите время в секундах, по прошествии которого сетевой интерфейс должен начинать взаимодействовать с модемом. Максимальное значение: 30. Параметр используется, когда загрузка модема занимает слишком много времени.

13. При необходимости укажите сетевой режим для сетевого интерфейса, выполнив следующие действия:

    a. В блоке **Режимы** нажмите на кнопку **+ Добавить**.

    b. В раскрывающемся списке выберите одно из следующих значений:

       - **All** – использовать все доступные сетевые режимы.
       - **LTE**.
       - **UMTS**.
       - **GSM**.
       - **CDMA**.
       - **TD-SCDMA**.

    Сетевой режим будет указан и отобразится в блоке **Режимы**. Вы можете указать несколько сетевых режимов и удалить режим, нажав рядом с ним на значок удаления ✕.

14. В поле **Профиль подключения** введите индекс профиля подключения, который сетевой интерфейс должен использовать вместо идентификатора APN. Максимальная длина: 30 символов.

15. В раскрывающемся списке **IP-стек** выберите IP-стек, который должен использоваться на сетевом интерфейсе:

- **IPv4 –** использовать на сетевом интерфейсе стек протокола IPv4. Значение по умолчанию.
- **IPV6 –** использовать на сетевом интерфейсе стек протокола IPv6.
- **Двойной стек (IPv4 и IPv6) –** использовать на сетевом интерфейсе двойной стек IPv4 и IPv6.

16. Снимите флажок **IPv4 через DHCP**, чтобы не назначать сетевому интерфейсу IPv4-адрес по протоколу DHCP. При необходимости установить этот флажок одновременно с флажком **IPv6 через DHCP** в раскрывающемся списке **IP-стек** выберите **Двойной стек (IPv4 и IPv6)**. По умолчанию флажок установлен.

17. Установите флажок **IPv6 через DHCP**, чтобы назначить сетевому интерфейсу IPv6-адрес по протоколу DHCP. При необходимости установить этот флажок одновременно с флажком **IPv4 через DHCP** в раскрывающемся списке **IP-стек** выберите **Двойной стек (IPv4 и IPv6)**. По умолчанию флажок снят.

18. Снимите флажок **Автоподключение**, чтобы не подключать автоматически модем к сети. По умолчанию флажок установлен.

19. В поле **PLMN** введите идентификатор PLMN оператора связи. Первые три цифры идентификатора PLMN являются кодом страны, а вторые три цифры – кодом мобильной сети.

20. В поле **Время** введите время в секундах для ожидания сетевым интерфейсом выполнения операций на SIM-карте, установленной в модеме. Максимальное значение: 20. По умолчанию указано значение `10`.

21. В поле **Серийный номер** введите последовательный порт (англ. serial port) модема. Максимальная длина: 50 символов.

22. Если вы создаете первый сетевой интерфейс, на который будет ссылаться интерфейс SD-WAN с типом WAN, в поле **Метрика маршрута** введите `100`. Для каждого следующего сетевого интерфейса, на который будет ссылаться интерфейс SD-WAN с типом WAN, требуется увеличить значение на 1. Например, для второго сетевого интерфейса введите `101`.

23. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

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

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.
   - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**.

   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 этот псевдоним при создании интерфейса SD-WAN с типом WAN. Максимальная длина: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите ранее созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина: 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 раскрывающемся списке **Протокол** выберите **PPPoE**.

7. В поле **Концентратор доступа** введите IP-адрес или имя хоста концентратора доступа, к которому должен подключиться сетевой интерфейс. Максимальная длина: 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 должен подключиться сетевой интерфейс. Максимальная длина: 30 символов. Если вы не вводите значение в этом поле, PPPD использует первый обнаруженный 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: 30 символов.

     b. В поле **Пароль для аутентификации PAP/CHAP** введите пароль для PAP/CHAP-аутентификации. Максимальная длина: 30 символов.

   - **Отсутствует** – на сетевом интерфейсе не используется аутентификация.

10. В поле **Максимум неудачных пингов** введите количество безуспешных ICMP-запросов, при котором сетевой интерфейс должен считать PPPoE-сервер недоступным. Диапазон значений: от 1 до 3600. По умолчанию указано значение `5`.

11. В поле **Интервал пингов (сек.)** введите интервал в секундах для отправки сетевым интерфейсом ICMP-запросов PPoE-серверу. Диапазон значений: от 1 до 3600. По умолчанию указано значение `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: 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. Если вы создаете первый сетевой интерфейс, на который будет ссылаться интерфейс SD-WAN с типом WAN, в поле **Метрика маршрута** введите `100`. Для каждого следующего сетевого интерфейса, на который

будет ссылаться интерфейс SD-WAN с типом WAN, требуется увеличить значение на 1. Например, для второго сетевого интерфейса введите `101`.

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 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 PPPD (Point-to-Point Protocol Daemon) при запуске, 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, выполнив следующие действия:

    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 сервер, нажав рядом с ним на значок удаления ✕.

19. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

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

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.
    - Если вы хотите создать сетевой интерфейс на устройстве CPE, перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**.

    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 этот псевдоним при создании интерфейса SD-WAN с типом WAN. Максимальная длина: 15 символов.

4. Если вы хотите добавить сетевой интерфейс в зону межсетевого экрана, в раскрывающемся списке **Зона** выберите ранее созданную зону межсетевого экрана.

5. В поле **Имя интерфейса** введите имя физического порта или виртуального интерфейса операционной системы устройства CPE. Максимальная длина: 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. Если вы хотите создать мост из физических или виртуальных интерфейсов, имена которых указаны в поле **Имя интерфейса**, выполните следующие действия:

   a. Установите флажок **Мост**. По умолчанию флажок снят.

   b. Если вы хотите использовать на мосту протокол STP для предотвращения петель маршрутизации, установите флажок **STP**. По умолчанию флажок снят.

   c. В поле **Возраст (сек.)** введите время в секундах, в течение которого динамические записи должны храниться 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**. По умолчанию флажок снят.

8. В раскрывающемся списке **Протокол** выберите **Отсутствует**.

9. Если вы хотите, чтобы сетевой интерфейс автоматически включался одновременно с устройством CPE, установите флажок **Включать автоматически**. По умолчанию флажок снят.

10. Если вы хотите, чтобы сетевому интерфейсу автоматически назначался IP-адрес, маршрут и шлюз по умолчанию, установите флажок **Назначать IP, маршрут и шлюз**. По умолчанию флажок снят.

11. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет фактический MAC-адрес сетевого интерфейса.

12. В поле **Переопределить MTU** введите значение MTU для сетевого интерфейса. Введенное значение заменяет MTU по умолчанию.

13. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

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

Изменение сетевого интерфейса

Вы можете изменить сетевой интерфейс в шаблоне CPE или на устройстве. Когда вы изменяете сетевой интерфейс в шаблоне CPE, этот интерфейс автоматически изменяется на всех использующих шаблон устройствах. Описание параметров см. в инструкциях по созданию сетевого интерфейса.

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.

   - Если вы хотите изменить сетевой интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**. Если вы хотите изменить сетевой интерфейс, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с этим сетевым интерфейсом.

   Отобразится таблица сетевых интерфейсов.

2. Нажмите на кнопку **Изменить** рядом с сетевым интерфейсом, который вы хотите изменить.

3. В открывшемся окне измените параметры сетевого интерфейса.

4. Нажмите на кнопку **Сохранить**.

   Сетевой интерфейс будет изменен и обновится в таблице.

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

Выключение и включение сетевого интерфейса

Вы можете выключить или включить сетевой интерфейс в шаблоне CPE или на устройстве. Когда вы выключаете или включаете сетевой интерфейс в шаблоне CPE, этот интерфейс автоматически выключается или включается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.

   - Если вы хотите выключить или включить сетевой интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**. Если вы хотите выключить или включить сетевой интерфейс, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с этим 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

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 → Устройства CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, к которому вы хотите не применять параметры сетевых интерфейсов.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Установите флажок **Игнорировать параметры сети**. По умолчанию флажок снят.

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. Когда вы удаляете сетевой интерфейс в шаблоне CPE, этот интерфейс автоматически удаляется на всех использующих шаблон устройствах. Вы не можете удалить на устройстве CPE сетевой интерфейс, унаследованный из шаблона.

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 и в отобразившейся области настройки выберите вкладку **Параметры сети**.
   - Если вы хотите удалить сетевой интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры сети**.

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

Настройка подключения устройства CPE к оркестратору и контроллеру

При регистрации устройство CPE подключается к оркестратору и контроллеру. Вы можете настроить подключение в шаблоне CPE. Когда вы настраиваете подключение в шаблоне CPE, указанные параметры автоматически распространяются на все использующие шаблон устройства.

Определенные параметры подключения можно также настроить на устройстве CPE, например, включить автоматическую перезагрузку при разрыве управляющей сессии с контроллером.

Чтобы настроить подключение устройства CPE к оркестратору и контроллеру:

1. Перейдите к настройке подключения 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 и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN → Общие параметры**.

   - Если вы хотите настроить подключение к оркестратору и контроллеру на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите устройство, в отобразившейся области настройки выберите вкладку **Параметры SD-WAN → Общие параметры** и установите флажок **Переопределить**.

   Отобразятся параметры подключения к оркестратору и контроллеру.

2. Если вы настраиваете подключение к оркестратору и контроллеру в шаблоне CPE, выполните следующие действия:

   a. В поле **IP/FQDN оркестратора** введите IP-адрес или FQDN оркестратора. Максимальная длина: 50 символов.

   b. В раскрывающемся списке **Протокол оркестратора** выберите протокол подключения устройства CPE к оркестратору:

      - **http**;

      - **https** – значение по умолчанию.

   c. В поле **Порт оркестратора** введите номер порта оркестратора. Диапазон значений: от 0 до 65 535.

   d. В раскрывающемся списке **OpenFlow-транспорт** выберите, должна ли шифроваться управляющая сессия между устройством CPE и контроллером:

      - **TCP** – не шифровать управляющую сессию.

      - **SSL** – шифровать управляющую сессию. Значение по умолчанию.

Эти параметры можно указать только в шаблоне CPE. Остальные параметры в этой инструкции можно настроить в шаблоне CPE и на устройстве.

3. В раскрывающемся списке **Автоперезагрузка** выберите, должно устройство CPE автоматически перезагружаться при потере связи с контроллером:

   - **Да**. При выборе этого значения в поле **Время перезагрузки (сек.)** введите время в секундах, по прошествии которого устройство CPE должно автоматически перезагрузиться при потере связи с контроллером. Диапазон значений: от 60 до 2 073 600.

   - **Нет** – значение по умолчанию.

4. В раскрывающемся списке **Приоритетный интерфейс управления** выберите, как определяется новая основная управляющая сессия между устройством CPE и контроллером при разрыве предыдущей сессии:

   - **Случайно** – новой управляющей основной сессией становится сессия, установленная со случайно выбранного интерфейса SD-WAN с типом WAN устройства CPE. Значение по умолчанию.

   - **<интерфейс SD-WAN>** – новой основной управляющей сессией становится сессия, установленная с указанного интерфейса SD-WAN с типом WAN устройства CPE. Если интерфейс недоступен, новой основной управляющей сессией становится сессия, установленная со случайно выбранного интерфейса.

     При выборе этого значения, если вы хотите, чтобы при восстановлении предыдущая основная управляющая сессия снова становилась основной, выполните следующие действия:

     a. Установите флажок **Обратное переключение**. По умолчанию флажок снят.

     b. В поле **Время** введите время в секундах, по прошествии которого восстановленная управляющая сессия должна стать основной. Диапазон значений: от 0 до 86 400.

5. В поле **Интервал обновления (сек.)** введите интервал в секундах для отправки устройством CPE REST API-запросов оркестратору. Диапазон значений: от 5 до 300. По умолчанию указано значение `30`.

6. В поле **URL ZTP** 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.

   - Вам нужно указать `http` или `https`.

   По умолчанию используется шаблон `http://192.168.7.1/cgi-bin/config?payload={config}`.

7. В поле **Интерактивный интервал обновления (сек.)** введите интервал 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.

8. В поле **Таймаут интерактивного режима (сек.)** введите время в секундах, по прошествии которого на устройстве CPE должен автоматически выключиться интерактивный режим. Диапазон значений: от 30 до 180.

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

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 – интерфейсы SD-WAN, ссылающиеся на сетевые интерфейсы, которые подключены к LAN. Эти интерфейсы созданы по умолчанию, и вы не можете удалять и создавать их. Вы можете изменить интерфейсы SD-WAN с типом LAN, 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 – 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 SSH. Этот интерфейс создан по умолчанию, и вы не можете удалить его или создать новые интерфейсы. Если вы не хотите использовать интерфейс SD-WAN с типом management, вы можете его выключить.

Таблица интерфейсов SD-WAN отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы интерфейсов SD-WAN в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Параметры SD-WAN → Интерфейсы**.

- Для отображения таблицы интерфейсов SD-WAN на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Параметры SD-WAN → Интерфейсы**.

Информация об интерфейсах SD-WAN отображается в следующих столбцах таблицы:

- **Тип** – тип интерфейса SD-WAN:
  - **WAN**.
  - **LAN**.
  - **Management**.
- **Унаследовано** – унаследован ли интерфейс SD-WAN 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 мегабит 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** – интервал проверки WAN в секундах.
- **Down** – количество безуспешных проверок для признания WAN недоступной.
- **Up** – количество успешных проверок для признания WAN доступной.
- **Мониторинг скорости** – измеряется ли скорость интерфейса SD-WAN с типом WAN:
  - **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.

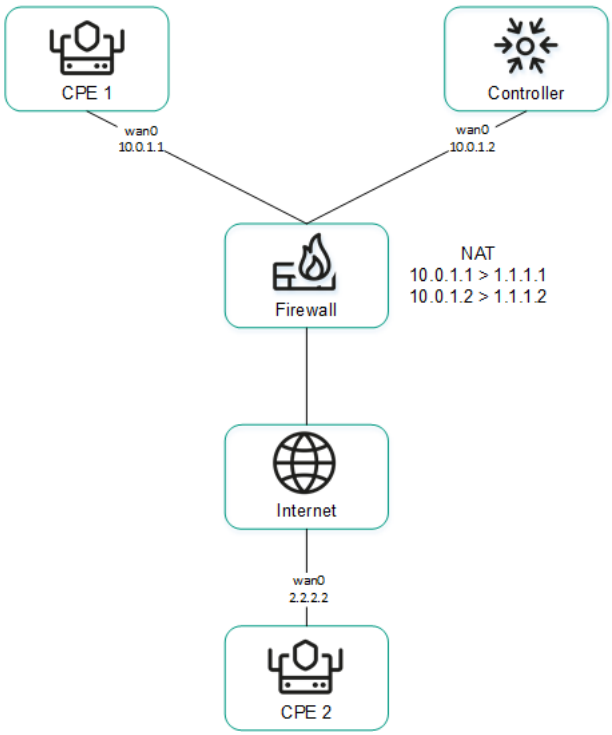
Передача контроллеру публичных IP-адресов и UDP-портов интерфейсов SD-WAN с типом WAN

Для построения GENEVE-туннелей 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 и передать его другим устройствам в топологии (устройство CPE 2).

В результате между устройствами CPE 1 и 2 невозможно построить GENEVE-туннель, 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

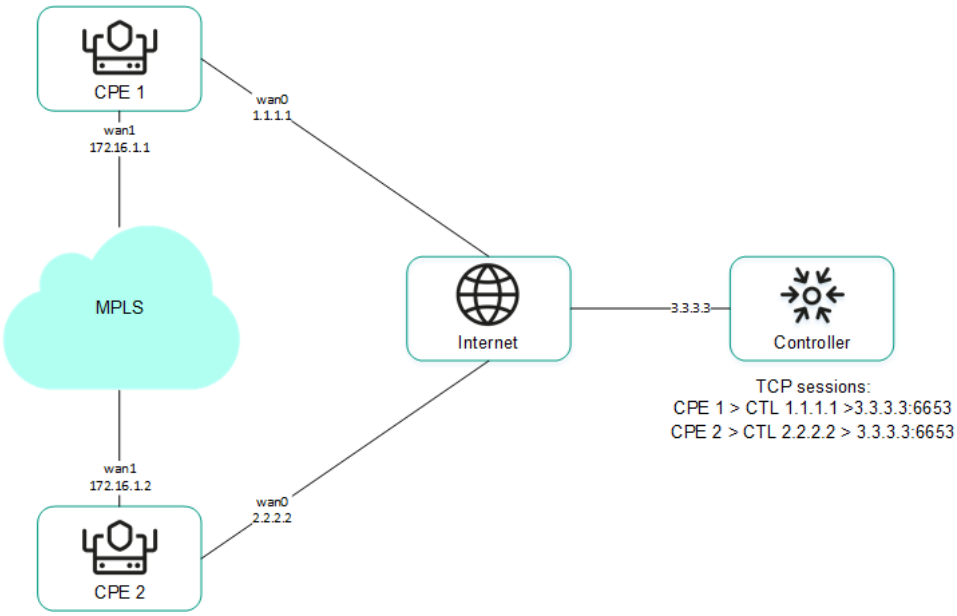
Передача контроллеру IP-адресов интерфейсов SD-WAN с типом WAN, находящихся в изолированной сети

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 GENEVE-туннелей. В этом случае контроллер не может получить информацию об IP-адресах изолированных интерфейсов и использовать ее для построения GENEVE-туннелей 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 интерфейсы wan0, так как интерфейсы wan1 находятся в изолированной сети (MPLS), которая не имеет доступа к контроллеру. При этом оба интерфейса wan1 могут быть использованы, чтобы построить GENEVE-туннели.

Если у одного из устройств CPE выходит из строя канал для взаимодействия с контроллером, все остальные каналы также не могут быть использованы, даже если они сохраняют работоспособность, так как контроллер исключает устройство из топологии.

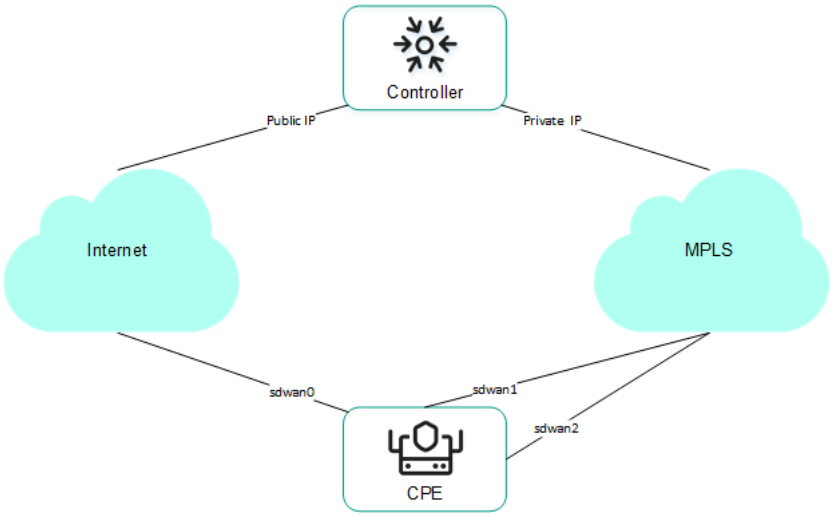
IP-адреса изолированных интерфейсов SD-WAN с типом WAN передаются контроллеру через оркестратор.



Устройства CPE 1`и 2 связаны друг с другом через MPLS, а также с контроллером через интернет

О переопределении IP-адреса и порта для подключения интерфейса SD-WAN с типом WAN к контроллеру

Вы можете подключить интерфейсы SD-WAN с типом WAN к контроллеру, даже если они используют разные типы каналов, например интернет и частную MPLS-сеть (см. рисунок ниже). Вам нужно вручную переопределить IP-адреса и порты для подключения к контроллеру при создании или изменении интерфейса SD-WAN с типом WAN.



Подключение устройства CPE к контроллеру через два разных канала связи

Если в вашем экземпляре SD-WAN используется несколько узлов контроллера, вам нужно переопределить IP-адреса для всех узлов. При несовпадении количества узлов контроллера с количеством указанных IP-адресов происходит ошибка и данные остаются прежними.

Вам нужно перезагрузить устройство CPE после переопределения IP-адреса и порта для подключения интерфейса SD-WAN с типом WAN к контроллеру.

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, или в файле настройки контроллера.

Отправленные ICMP-запросы имеют размер пакета 1600 байт. Если хотя бы один из этих запросов получает ответ, проверка фрагментации пакетов на устройстве CPE считается успешной. Вы можете просмотреть результат проверки фрагментации в столбце **Фрагментация** таблицы устройств CPE или таблицы каналов.

Создание интерфейса SD-WAN с типом WAN

Вы можете создать интерфейс SD-WAN с типом WAN в шаблоне CPE или на устройстве. Когда вы создаете интерфейс SD-WAN с типом WAN в шаблоне CPE, этот интерфейс автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN** → **Интерфейсы**.

   - Если вы хотите создать интерфейс SD-WAN с типом WAN на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN** → **Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

2. Нажмите на кнопку **+ Интерфейс SD-WAN**.

3. В открывшемся окне в поле **OpenFlow-интерфейс** введите номер OpenFlow-порта, который должен быть создан на виртуальном коммутаторе.

4. В поле **Интерфейс (псевдоним)** введите имя ранее созданного сетевого интерфейса, на который интерфейс SD-WAN с типом WAN должен ссылаться.

5. В поле **Максимальная скорость** введите максимальную скорость интерфейса SD-WAN с типом WAN в мегабит в секунду. Диапазон значений: от 1 до 100 000. По умолчанию указано значение `1000`.

6. Настройте проверку доступности WAN, к которой подключен интерфейс SD-WAN с типом WAN, выполнив следующие действия:

   a. Укажите хоста для проверки доступности WAN, выполнив следующие действия:

      1. В блоке **IP для отслеживания** в отображающемся поле введите IP-адрес хоста.

      2. Нажмите на кнопку **+ Добавить**.

      Хост будет указан и отобразится в блоке **IP для отслеживания**. Вы можете указать несколько хостов и удалить хост, нажав рядом с ним на значок удаления ✕.

b. В поле **IP для проверки фрагментации** введите IPv4-адрес хоста, до которого должна проверяться поддержка фрагментации. Значение по умолчанию: 1.1.1.1.

c. В поле **Надежность** введите минимальное количество успешных проверок для признания WAN доступной. По умолчанию указано значение `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** введите интервал проверки WAN в секундах. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

e. В поле **Количество** введите количество запросов хостам в рамках одной проверки WAN. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

f. В поле **Время** введите время ожидания ответа от хостов в миллисекундах. Диапазон значений: от 1 до 100 000. По умолчанию указано значение `2000`.

g. В поле **Down** введите количество безуспешных проверок для признания WAN недоступной. Диапазон значений: от 1 до 600. По умолчанию указано значение `3`.

h. В поле **Up** введите количество успешных проверок для признания WAN доступной. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

i. В раскрывающемся списке **Мониторинг скорости** выберите, должна ли измеряться скорость интерфейса SD-WAN с типом WAN:

- **Да**.
- **Нет** – значение 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 WAN-сети**.

b. В раскрывающемся списке **Состояние** выберите одно из следующих значений:

- **Выключено** – контроллеру не требуется передавать информацию об интерфейсе SD-WAN с типом WAN.
- **NAT/PAT** – интерфейс SD-WAN с типом WAN находится за NAT или PAT, и ему требуется назначить публичный IP-адрес и номер UDP-порта, после чего передать их контроллеру.
- **Изолированные WAN-сети** – интерфейс SD-WAN с типом WAN подключен к изолированной сети и его IP-адрес требуется передать контроллеру.

c. Если в раскрывающемся списке **Состояние** вы выбрали **NAT/PAT**, выполните следующие действия:

1. В поле **Публичный IP** введите публичный IPv4-адрес интерфейса SD-WAN с типом WAN.
2. В поле **Публичный 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 **Изолированные WAN-сети**, в поле **IP-адрес** введите IPv4-адрес интерфейса SD-WAN с типом WAN.

9. Если вы хотите переопределить IP-адрес и порт для подключения интерфейса SD-WAN с типом WAN к контроллеру, выполните следующие действия:

a. Выберите вкладку **Контроллеры**.

b. Установите флажок **Переписать IP/порт контроллеров**. По умолчанию флажок снят.

c. В раскрывающемся списке **Количество контроллеров** выберите количество узлов контроллера в экземпляре SD-WAN.

Вам нужно переопределить IP-адрес для подключения интерфейса SD-WAN с типом WAN к каждому узлу контроллера. В противном случае происходит ошибка и данные остаются прежними.

d. В поле **IP-адрес** введите IPv4-адрес для подключения интерфейса SD-WAN с типом WAN к контроллеру. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**.

e. В поле **Порт** введите номер стартового порта для подключения интерфейса SD-WAN с типом WAN к контроллеру. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**. Диапазон значений: от 1 до 65 535. По умолчанию введено значение `6653`.

Количество определяемых портов зависит от количества интерфейсов SD-WAN с типом WAN устройства CPE. Например, если вы вводите номер стартового порта `6653`, и устройство имеет четыре интерфейса SD-WAN с типом WAN, на основании этого порта также определяются порты 6654, 6655 и 6656.

Вам нужно перезагрузить устройство CPE после переопределения IP-адреса и порта для подключения интерфейса SD-WAN с типом WAN к контроллеру.

10. Нажмите на кнопку **Создать**.

Интерфейс SD-WAN с типом WAN будет создан и отобразится в таблице.

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

Изменение интерфейса SD-WAN с типом WAN

Вы можете изменить интерфейс SD-WAN с типом WAN в шаблоне CPE или на устройстве. Вы не можете изменить имя интерфейса SD-WAN с типом WAN. Когда вы изменяете интерфейс SD-WAN с типом WAN в шаблоне CPE, этот интерфейс автоматически изменяется на всех использующих шаблон устройствах.

Чтобы изменить интерфейс SD-WAN с типом WAN:

1. Перейдите к изменению интерфейса SD-WAN с типом WAN одним из следующих способов:

   - Если вы хотите изменить интерфейс SD-WAN с типом WAN в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   - Если вы хотите изменить интерфейс SD-WAN с типом WAN на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN → Интерфейсы**. Если вы хотите изменить интерфейс SD-WAN с типом WAN, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с этим интерфейсом.

   Отобразится таблица интерфейсов SD-WAN.

2. Нажмите на кнопку **Изменить** рядом с интерфейсом SD-WAN с типом WAN, который вы хотите изменить.

3. В открывшемся окне в поле **OpenFlow-интерфейс** введите номер OpenFlow-порта, который должен быть создан на виртуальном коммутаторе.

4. В поле **Максимальная скорость** введите максимальную скорость интерфейса SD-WAN с типом WAN в мегабит в секунду. Диапазон значений: от 1 до 100 000. По умолчанию указано значение `1000`.

5. Настройте проверку доступности WAN, к которой подключен интерфейс SD-WAN с типом WAN, выполнив следующие действия:

   a. Укажите хоста для проверки доступности WAN, выполнив следующие действия:

      1. В блоке **IP для отслеживания** в отображающемся поле введите IP-адрес хоста.

      2. Нажмите на кнопку **+ Добавить**.

      Хост будет указан и отобразится в блоке **IP для отслеживания**. Вы можете указать несколько хостов и удалить хост, нажав рядом с ним на значок удаления ✕.

   b. В поле **IP для проверки фрагментации** введите IPv4-адрес хоста, до которого должна проверяться поддержка фрагментации. Значение по умолчанию: 1.1.1.1.

   c. В поле **Надежность** введите минимальное количество успешных проверок для признания WAN доступной. По умолчанию указано значение `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** введите интервал проверки WAN в секундах. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

e. В поле **Количество** введите количество запросов хостам в рамках одной проверки WAN. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

f. В поле **Время** введите время ожидания ответа от хостов в миллисекундах. Диапазон значений: от 1 до 100 000. По умолчанию указано значение `2000`.

g. В поле **Down** введите количество безуспешных проверок для признания WAN недоступной. Диапазон значений: от 1 до 600. По умолчанию указано значение `3`.

h. В поле **Up** введите количество успешных проверок для признания WAN доступной. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

i. В раскрывающемся списке **Мониторинг скорости** выберите, должна ли измеряться скорость интерфейса SD-WAN с типом WAN:

- **Да**.
- **Нет** – значение по умолчанию.

6. 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.

7. Если вы хотите настроить передачу контроллеру информации об интерфейсе SD-WAN с типом WAN, выполните следующие действия:

a. Выберите вкладку **NAT и изолированные WAN-сети**.

b. В раскрывающемся списке **Состояние** выберите одно из следующих значений:

- **Выключено** – контроллеру не требуется передавать информацию об интерфейсе SD-WAN с типом WAN.
- **NAT/PAT** – интерфейс SD-WAN с типом WAN находится за NAT или PAT, и ему требуется назначить публичный IP-адрес и номер UDP-порта, после чего передать их контроллеру.

- **Изолированные WAN-сети** – интерфейс SD-WAN с типом WAN подключен к изолированной сети и его IP-адрес требуется передать контроллеру.

c. Если в раскрывающемся списке **Состояние** вы выбрали **NAT/PAT**, выполните следующие действия:

1. В поле **Публичный IP** введите публичный IPv4-адрес интерфейса SD-WAN с типом WAN.

2. В поле **Публичный 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 **Изолированные WAN-сети**, в поле **IP-адрес** введите IPv4-адрес интерфейса SD-WAN с типом WAN.

8. Если вы хотите переопределить IP-адрес и порт для подключения интерфейса SD-WAN с типом WAN к контроллеру, выполните следующие действия:

a. Выберите вкладку **Контроллеры**.

b. Установите флажок **Переписать IP/порт контроллеров**. По умолчанию флажок снят.

c. В раскрывающемся списке **Количество контроллеров** выберите количество узлов контроллера в экземпляре SD-WAN.

Вам нужно переопределить IP-адрес для подключения интерфейса SD-WAN с типом WAN к каждому узлу контроллера. В противном случае происходит ошибка и данные остаются прежними.

d. В поле **IP-адрес** введите IPv4-адрес для подключения интерфейса SD-WAN с типом WAN к контроллеру. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**.

e. В поле **Порт** введите номер стартового порта для подключения интерфейса SD-WAN с типом WAN к контроллеру. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**. Диапазон значений: от 1 до 65 535. По умолчанию введено значение `6653`.

Количество определяемых портов зависит от количества интерфейсов SD-WAN с типом WAN устройства CPE. Например, если вы вводите номер стартового порта `6653`, и устройство имеет четыре интерфейса SD-WAN с типом WAN, на основании этого порта также определяются порты 6654, 6655 и 6656.

Вам нужно перезагрузить устройство CPE после переопределения IP-адреса и порта для подключения интерфейса SD-WAN с типом WAN к контроллеру.

9. Нажмите на кнопку **Сохранить**.

Интерфейс SD-WAN с типом WAN будет изменен и обновится в таблице.

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

Изменение интерфейса SD-WAN с типом LAN

Вы можете изменить интерфейс SD-WAN с типом LAN в шаблоне CPE или на устройстве. Когда вы изменяете интерфейс SD-WAN с типом LAN в шаблоне CPE, этот интерфейс автоматически изменяется на всех использующих шаблон устройствах. При изменении интерфейса SD-WAN с типом LAN вы можете только указать максимальную скорость и настроить очереди трафика.

Чтобы изменить интерфейс SD-WAN с типом LAN:

1. Перейдите к изменению интерфейса SD-WAN с типом LAN одним из следующих способов:

   - Если вы хотите изменить интерфейс SD-WAN с типом LAN в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   - Если вы хотите изменить интерфейс SD-WAN с типом LAN на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN → Интерфейсы**. Если вы хотите изменить интерфейс SD-WAN с типом LAN, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с этим интерфейсом.

   Отобразится таблица интерфейсов SD-WAN.

2. Нажмите на кнопку **Изменить** рядом с интерфейсом SD-WAN с типом LAN, который вы хотите изменить.

3. В открывшемся окне в поле **Максимальная скорость** введите максимальную скорость интерфейса SD-WAN в мегабит в секунду. Диапазон значений: от 1 до 100 000. По умолчанию указано значение `1000`.

4. Если вы хотите настроить очереди трафика на интерфейсе SD-WAN с типом LAN, выполните следующие действия:

   a. Выберите вкладку **QoS**.

      Отобразится таблица очередей трафика.

   b. В столбце **Минимальная скорость (%)** укажите минимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN с типом LAN. Сумма значений в столбце не должна превышать 100.

   c. В столбце **Максимальная скорость (%)** укажите максимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN с типом LAN. 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 LAN указывается на шаге 3 этой инструкции.

5. Нажмите на кнопку **Сохранить**.

   Интерфейс SD-WAN с типом LAN будет изменен и обновится в таблице.

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

Выключение и включение интерфейса SD-WAN

Вы можете выключить или включить интерфейс SD-WAN в шаблоне CPE или на устройстве. Когда вы выключаете или включаете интерфейс SD-WAN в шаблоне CPE, этот интерфейс автоматически выключается или включается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN** → **Интерфейсы**.

   - Если вы хотите выключить или включить интерфейс SD-WAN на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN** → **Интерфейсы**. Если вы хотите выключить или включить интерфейс SD-WAN, унаследованный из шаблона CPE, установите флажок **Переопределить** рядом с этим интерфейсом.

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

Удаление интерфейса SD-WAN с типом WAN

Вы можете удалить интерфейс SD-WAN с типом WAN в шаблоне CPE или на устройстве. Когда вы удаляете интерфейс SD-WAN с типом WAN в шаблоне CPE, этот интерфейс автоматически удаляется на всех использующих шаблон устройствах. Вы не можете удалить на устройстве CPE интерфейс SD-WAN, унаследованный из шаблона.

Удаление интерфейсов SD-WAN с типом LAN не поддерживается.

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 и в отобразившейся области настройки выберите вкладку **Параметры SD-WAN** → **Интерфейсы**.

   - Если вы хотите удалить интерфейс SD-WAN с типом WAN на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Параметры 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

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 этот сервисный интерфейс. ACL-интерфейс применяет к сервисному интерфейсу указанный фильтр трафика. На один сервисный интерфейс могут ссылаться не более четырех ACL-интерфейсов.

Для отображения таблицы сервисных интерфейсов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE, и в открывшемся меню настройки контроллера 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 типом инкапсуляции **VLAN** и **Q-in-Q**.
- **Внутренний VLAN** – внутренняя метка VLAN сервисного интерфейса. Значение в этом столбце отображается только для сервисных интерфейсов с типом инкапсуляции **Q-in-Q**.
- **Фильтр** – фильтр трафика для ACL-интерфейса. Значение в этом столбце отображается только для сервисных интерфейсов с типом инкапсуляции **ACL**.
- **Имя** – имя сервисного интерфейса.

Действия, которые вы можете выполнить с таблицей, описаны в инструкции 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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 сервисный интерфейс должен ссылаться.

5. Нажмите на кнопку **Создать сервисный интерфейс**.

6. В открывшемся окне в раскрывающемся списке **Тип** выберите тип классификации трафика на сервисном интерфейсе:

   - **Access** – значение 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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 ранее 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 ACL-интерфейс должен ссылаться.

8. В раскрывающемся списке **Фильтр трафика** выберите ранее 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, этот 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

Вы можете просмотреть, какие транспортные сервисы используют сервисный интерфейс или ACL-интерфейс. Если сервисный интерфейс или ACL-интерфейс используется хотя бы одним транспортным сервисом, этот интерфейс невозможно удалить.

Чтобы просмотреть использование сервисного интерфейса или ACL-интерфейса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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 просмотреть.

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. Вам нужно просмотреть использование сервисного интерфейса или ACL-интерфейса и убедиться, что он не используется ни одним транспортным сервисом.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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 SD-WAN использует OpenFlow-порты, чтобы управлять трафиком сети. Поверх OpenFlow-портов можно создавать сервисные интерфейсы и UNI.

Вы можете объединить OpenFlow-порты в группы и использовать их при создании транспортных сервисов M2M и P2M. Когда вы добавляете группу OpenFlow-портов в транспортный сервис, поверх каждого порта в группе автоматически создается сервисный интерфейс, который используется транспортным сервисом. Использование групп OpenFlow-портов избавляет вас от необходимости вручную создавать сервисные интерфейсы и добавлять их в транспортные сервисы.

Для отображения таблицы групп OpenFlow-портов вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE, и в открывшемся меню настройки контроллера перейти в раздел **OpenFlow-группы**. Информация о группах OpenFlow-портов отображается в следующих столбцах таблицы:

- **Имя** – имя группы OpenFlow-портов.

- **Порты** – OpenFlow-порты, добавленные в группу.

Действия, которые вы можете выполнить с таблицей, описаны в инструкции 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **OpenFlow-группы**.

   Отобразится таблица групп OpenFlow-портов.

4. В верхней части страницы нажмите на кнопку **+ OpenFlow-группа**.

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. Вы можете добавить несколько OpenFlow-портов в группу.

7. Нажмите на кнопку **Создать**.

Группа OpenFlow-интерфейсов 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **OpenFlow-группы**.

   Отобразится таблица групп OpenFlow-портов.

4. Нажмите на кнопку **Управление** → **Изменить** рядом с группой OpenFlow-портов, которую вы хотите изменить.

5. В открывшемся окне в поле **Имя** введите имя группы OpenFlow-интерфейсов.

6. При необходимости в раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-порт, который вы хотите добавить в группу. Вы можете добавить несколько OpenFlow-портов в группу.

7. 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключено устройство CPE.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **OpenFlow-группы**.

   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.

Вам нужно создать UNI в шаблоне UNI, после чего применить его к устройствам CPE при добавлении или ручной регистрации, чтобы не создавать UNI на каждом отдельном устройстве. Если вы изменяете UNI в шаблоне, этот UNI автоматически изменяется на всех использующих шаблон устройствах CPE.

При создании UNI для него автоматически создается сервисный интерфейс.

Работа с шаблонами UNI

Таблица шаблонов UNI отображается в разделе **SD-WAN → Шаблоны UNI**. Информация о шаблонах UNI отображается в следующих столбцах таблицы:

- **ID** – идентификатор шаблона UNI.
- **Имя** – имя шаблона UNI.
- **Используется** – используется ли шаблон UNI 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 инструкции Работа с таблицами компонентов решения.

Параметры шаблона UNI отображаются на следующих вкладках:

- **Информация** – основная информация о шаблоне UNI. Вы можете изменить имя шаблона в поле **Имя**.
- **UNI** – UNI, созданные в шаблоне.

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.

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.

   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 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 отображения таблицы UNI в шаблоне UNI вам нужно в меню перейти в раздел **SD-WAN → Шаблоны UNI**, нажать на шаблон UNI и в отобразившейся области настройки выбрать вкладку **UNI**. Информация о UNI отображается в следующих столбцах таблицы:

- **Имя** – имя UNI.
- **OpenFlow-интерфейс** – номер OpenFlow-порта, на который ссылается UNI.
- **Инкапсуляция** – тип классификации трафика на UNI:
  - **Access**.
  - **VLAN**.
  - **Q-in-Q**.
- **Действия** – действия, которые можно выполнить с UNI.

Работа с UNI на устройстве CPE

Для отображения списка UNI на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **UNI**.

Создание UNI

Вы можете создать UNI в шаблоне UNI или на устройстве CPE. Когда вы создаете UNI в шаблоне UNI, этот UNI автоматически создается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **UNI**.
- Если вы хотите создать UNI на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки 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 UNI должен ссылаться, одним из следующих способов:
   - Если вы создаете UNI в шаблоне UNI, в поле **OpenFlow-интерфейс** введите номер OpenFlow-порта.
   - Если вы создаете UNI на устройстве CPE, в раскрывающемся списке **Порт** выберите OpenFlow-порт.
5. В раскрывающемся списке **Инкапсуляция** выберите тип классификации трафика на UNI:
   - **Access** – значение 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 ранее 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

Вы можете просмотреть, какие сетевые сервисы используют UNI на устройстве CPE. Если UNI используется хотя бы одним сетевым сервисом, этот UNI невозможно удалить.

Чтобы просмотреть использование UNI:

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

   Отобразится таблица устройств CPE.
2. Нажмите на устройство CPE, на котором вы хотите просмотреть использование UNI.

В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 просмотреть.

Откроется окно с таблицей сетевых сервисов, использующих UNI.

Изменение UNI

Вы можете изменить UNI в шаблоне UNI. Когда вы изменяете UNI в шаблоне UNI, этот UNI изменяется на всех использующих шаблон устройствах CPE.

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.

   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 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 в поле **Имя** введите имя UNI.

6. В поле **OpenFlow-интерфейс** введите номер OpenFlow-порта, на который UNI должен ссылаться.

7. В раскрывающемся списке **Инкапсуляция** выберите тип инкапсуляции на UNI:

   - **Access** – значение 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.

8. Нажмите на кнопку **Сохранить**.

   UNI будет изменен и обновится в таблице.

9. 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. Когда вы удаляете UNI в шаблоне UNI, этот UNI автоматически удаляется на всех использующих шаблон устройствах CPE.

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.

   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 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. Вам нужно просмотреть использование UNI и убедиться, что он не используется ни одним сетевым сервисом.

Чтобы удалить UNI на устройстве CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите удалить UNI.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 и удаление 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.

Добавление статического маршрута

Вы можете добавить статический маршрут в шаблоне CPE или на устройстве. Когда вы добавляете статический маршрут в шаблоне CPE, этот статический маршрут автоматически добавляется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Статические маршруты**.

   - Если вы хотите добавить статический маршрут на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Статические маршруты** и установите флажок **Переопределить**.

   Отобразится таблица статических маршрутов.

2. Нажмите на значок добавления статического маршрута ＋.

3. В раскрывающемся списке **Интерфейс** выберите ранее созданный сетевой интерфейс источника статического маршрута.

4. В поле **Узел назначения** введите IPv4-адрес назначения статического маршрута.

5. При необходимости в поле **IPv4-маска** введите IPv4-адрес подсети назначения статического маршрута.

6. В поле **Шлюз** введите IP-адрес шлюза статического маршрута.

7. В поле **Метрика** введите метрику статического маршрута. По умолчанию указано значение `0`.

8. В поле **MTU** введите значение MTU статического маршрута.

9. В раскрывающемся списке **Тип** выберите тип статического маршрута:

- **unicast** – значение по умолчанию.
- **local**.
- **broadcast**.
- **multicast**.
- **unreachable**.
- **prohibit**.
- **blackhole**.
- **anycast**.

10. Если вы хотите поместить статический маршрут в виртуальную таблицу маршрутизации, в раскрывающемся списке **VRF** выберите ранее созданную виртуальную таблицу маршрутизации. Вам нужно поместить статический маршрут в виртуальную таблицу маршрутизации, в которую помещен сетевой интерфейс источника статического маршрута.

    Статический маршрут будет добавлен и отобразится в таблице.

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

Удаление статического маршрута

Вы можете удалить статический маршрут в шаблоне CPE или на устройстве. Когда вы удаляете статический маршрут в шаблоне CPE, этот статический маршрут автоматически удаляется на всех использующих шаблон устройствах.

Удаленные статические маршруты невозможно восстановить.

Чтобы удалить статический маршрут:

1. Перейдите к удалению статического маршрута одним из следующих способов:

    - Если вы хотите удалить статический маршрут в шаблоне CPE, в меню перейдите в раздел **SD-WAN → Шаблоны CPE**, нажмите на шаблон и в отобразившейся области настройки выберите вкладку **Статические маршруты**.
    - Если вы хотите удалить статический маршрут на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Статические маршруты** и установите флажок **Переопределить**.

    Отобразится таблица статических маршрутов.

2. Нажмите значок удаления — рядом со статическим маршрутом, который вы хотите удалить.

    Статический маршрут будет удален и перестанет отображаться в таблице.

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

Фильтрация маршрутов и пакетов трафика

Вы можете использовать следующие компоненты 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 диапазоны масок подсети. Вы можете использовать списки префиксов 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 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.

Работа со списками управления доступом (ACLs)

Таблица списков управления доступом отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы списков управления доступом в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Фильтры маршрутов** → **Списки управления доступом**.
- Для отображения таблицы списков управления доступом на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Фильтры маршрутов** → **Списки управления доступом**.

Информация о списках управления доступом отображается в следующих столбцах таблицы:

- **Имя** – имя списка управления доступом.
- **Унаследовано** – унаследован ли список управления доступом 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 должен применять правило.
- **Действие** – действие, которое правило должно выполнять 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. Когда вы создаете список управления доступом в шаблоне CPE, этот список автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Фильтры маршрутов → Списки управления доступом**.
   - Если вы хотите создать список управления доступом на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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: 50 символов. Не используйте пробелы в этом поле.
4. Создайте правило в списке управления доступом, выполнив следующие действия:

   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. Значение по умолчанию. При выборе этого значения в отобразившемся поле введите IPv4-префикс.

   d. В раскрывающемся списке **Действие** выберите действие, которое правило должно выполнять с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Значение по умолчанию.
      - **Отклонить** – запретить IPv4-префикс.

Правило будет создано. Вы можете добавить несколько правил и удалить правило, нажав рядом с ним на значок удаления ✕.

5. Нажмите на кнопку **Создать**.

   Список управления доступом будет создан и отобразится в таблице.

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

Изменение списка управления доступом

Вы можете изменить список управления доступом в шаблоне CPE или на устройстве. Когда вы изменяете список управления доступом в шаблоне CPE, этот список управления доступом автоматически изменяется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Фильтры маршрутов → Списки управления доступом**.

   - Если вы хотите изменить список управления доступом на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 в поле **Имя** введите имя списка управления доступом. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

4. Измените правило в списке управления доступом, выполнив следующие действия:

   a. 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.

   b. 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. Значение по умолчанию. При выборе этого значения в отобразившемся поле введите IPv4-префикс.

   c. В раскрывающемся списке **Действие** выберите действие, которое правило должно выполнять с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Значение по умолчанию.

      - **Отклонить** – запретить IPv4-префикс.

5. Если вы хотите создать правило в списке управления доступом, выполните следующие действия:

   a. Нажмите на кнопку **+ Правило**.

   b. Укажите параметры правила. Параметры правила описаны на шаге 4 этой инструкции.

   Правило будет создано. Вы можете добавить несколько правил и удалить правило, нажав рядом с ним на значок удаления ✕.

6. Нажмите на кнопку **Сохранить**.

   Список управления доступом будет изменен и обновится в таблице.

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

Удаление списка управления доступом

Вы можете удалить список управления доступом в шаблоне CPE или на устройстве. Когда вы удаляете список управления доступом в шаблоне CPE, этот список управления доступом автоматически удаляется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Фильтры маршрутов → Списки управления доступом**.

   - Если вы хотите удалить список управления доступом на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

Работа со списками префиксов (prefix lists)

Таблица списков префиксов отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы списков префиксов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Фильтры маршрутов → Списки префиксов**.

- Для отображения таблицы списков префиксов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Фильтры маршрутов → Списки префиксов**.

Информация о списках префиксов отображается в следующих столбцах таблицы:

- **Имя** – имя списка префиксов.

- **Унаследовано** – унаследован ли список префиксов 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 должен применять правило.

- **Действие** – действие, которое правило должно выполнять с IPv4-префиксом:

  - **Разрешить** – разрешить IPv4-префикс.

  - **Отклонить** – запретить IPv4-префикс.

- **Greater or equal** – начальное значение диапазона масок подсети, к которым список префиксов должен применять правило.

- **Less or equal** – конечное значение диапазона масок подсети, к которым список префиксов должен применять правило.

- **Управление** – действия, которые можно выполнить со списком префиксов.

Создание списка префиксов

Вы можете создать список префиксов в шаблоне CPE или на устройстве. Когда вы создаете список префиксов в шаблоне CPE, этот список автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки 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, в отобразившейся области настройки 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: 50 символов. Не используйте пробелы в этом поле.

4. Создайте правило в списке префиксов, выполнив следующие действия:

   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. Значение по умолчанию. При выборе этого значения в отобразившемся поле введите IPv4-префикс.

   d. В раскрывающемся списке **Действие** выберите действие, которое правило должно выполнять с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Значение по умолчанию.

      - **Отклонить** – запретить IPv4-префикс.

   e. В поле **Greater or equal** введите начальное значение диапазона масок подсети. Диапазон значений: от 0 до 32.

   f. В поле **Less or equal** введите конечное значение диапазона масок подсети. Диапазон значений: от 0 до 32.

   Правило будет создано. Вы можете добавить несколько правил и удалить правило, нажав рядом с ним на значок удаления ✕.

5. Нажмите на кнопку **Создать**.

   Список префиксов будет создан и отобразится в таблице.

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

Изменение списка префиксов

Вы можете изменить список префиксов в шаблоне CPE или на устройстве. Когда вы изменяете список префиксов в шаблоне CPE, этот список автоматически изменяется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки 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, в отобразившейся области настройки 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 в поле **Имя** введите имя списка префиксов. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

4. Измените правило в списке префиксов, выполнив следующие действия:

   a. 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.

   b. 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. Значение по умолчанию. При выборе этого значения в отобразившемся поле введите IPv4-префикс.

   c. В раскрывающемся списке **Действие** выберите действие, которое правило должно выполнять с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Значение по умолчанию.

      - **Отклонить** – запретить IPv4-префикс.

   d. В поле **Greater or equal** введите начальное значение диапазона масок подсети. Диапазон значений: от 0 до 32.

   e. В поле **Less or equal** введите конечное значение диапазона масок подсети. Диапазон значений: от 0 до 32.

5. Если вы хотите создать правило в списке префиксов, выполните следующие действия:

   a. Нажмите на кнопку **+ Правило**.

   b. Укажите параметры правила. Параметры правила описаны на шаге 4 этой инструкции.

   Правило будет создано. Вы можете добавить несколько правил и удалить правило, нажав рядом с ним на значок удаления ✕.

6. Нажмите на кнопку **Сохранить**.

   Список префиксов будет изменен и обновится в таблице.

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

Удаление списка префиксов

Вы можете удалить список префиксов в шаблоне CPE или на устройстве. Когда вы удаляете список префиксов в шаблоне CPE, этот список автоматически удаляется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Фильтры маршрутов → Списки префиксов**.

   - Если вы хотите удалить список префиксов на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

Работа с картами маршрутизации (route maps)

Таблица карт маршрутизации отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы карт маршрутизации в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Фильтры маршрутов → Карты маршрутизации**.

- Для отображения таблицы карт маршрутизации на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Фильтры маршрутов → Карты маршрутизации**.

Информация о картах маршрутизации отображается в следующих столбцах таблицы:

- **Имя** – имя карты маршрутизации.

- **Унаследовано** – унаследована ли карта маршрутизации 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 должно выполнять с IPv4-префиксом:
  - **Разрешить** – разрешить IPv4-префикс.
  - **Отклонить** – запретить IPv4-префикс.
- **Условие** – критерий, согласно которому карта маршрутизации должна применять правило IPv4-префиксу:
  - **Отсутствует** – применять правило ко всем IPv4-префиксам.
  - **Prefix-List** – применять правило к IPv4-префиксам, разрешенным указанным списком префиксов.
- **Значение** – список префиксов, который должен разрешить IPv4-префикс, чтобы карта маршрутизации применяла правило к этому IPv4-префиксу.
- **Изменить атрибут** – атрибут, значение которого правило должно изменять.
- **Новое значение** – значение, которое правило должно указывать для атрибута.
- **Управление** – действия, которые можно выполнить с картой маршрутизации.

Создание карты маршрутизации

Вы можете создать карту маршрутизации в шаблоне CPE или на устройстве. Когда вы создаете карту маршрутизации в шаблоне CPE, эта карта маршрутизации автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации**.
   - Если вы хотите создать карту маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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: 50 символов. Не используйте пробелы в этом поле.

4. Создайте правило в карте маршрутизации, выполнив следующие действия:

   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 должно выполнять с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Значение по умолчанию.
      - **Отклонить** – запретить IPv4-префикс.

   d. В раскрывающемся списке **Условие** выберите критерий, согласно которому карта маршрутизации должна применять правило к IPv4-префиксу:

      - **Отсутствует** – применять правило ко всем IPv4-префиксам. Значение по умолчанию.
      - **Prefix-List** – применять правило к IPv4-префиксам, разрешенным указанным списком префиксов. При выборе этого значения в раскрывающемся списке **Список префиксов** выберите ранее созданный список префиксов.

   e. Если в раскрывающемся списке **Условие** вы выбрали **Prefix-List**, в раскрывающемся списке **Изменить атрибут** выберите атрибут, который правило должно изменять:

      - **Отсутствует** – не изменять значения атрибутов. Значение 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 добавить несколько правил и удалить правило, нажав рядом с ним на значок удаления ✕.

5. Нажмите на кнопку **Создать**.

   Карта маршрутизации будет создана и отобразится в таблице.

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

Изменение карты маршрутизации

Вы можете изменить карту маршрутизации в шаблоне CPE или на устройстве. Когда вы изменяете карту маршрутизации в шаблоне CPE, эта карта автоматически изменяется на всех использующих шаблон устройствах.

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 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** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации** установите флажок **Переопределить**.

   Отобразится таблица карт маршрутизации.

2. Нажмите на кнопку **Изменить** рядом с картой маршрутизации, которую вы хотите изменить.

3. В открывшемся окне в поле **Имя** введите имя карты маршрутизации. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

4. Измените правило в карте маршрутизации, выполнив следующие действия:

   a. 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.

   b. В раскрывающемся списке **Действие** выберите действие, которое правило должно выполнять с IPv4-префиксом:

      - **Разрешить** – разрешить IPv4-префикс. Значение по умолчанию.

      - **Отклонить** – запретить IPv4-префикс.

   c. В раскрывающемся списке **Условие** выберите критерий, согласно которому карта маршрутизации должна применять правило к IPv4-префиксу:

      - **Отсутствует** – применять правило ко всем IPv4-префиксам. Значение по умолчанию.

      - **Prefix-List** – применять правило к IPv4-префиксам, разрешенным указанным списком префиксов. При выборе этого значения в раскрывающемся списке **Список префиксов** выберите ранее созданный список префиксов.

   d. Если в раскрывающемся списке **Условие** вы выбрали **Prefix-List**, в раскрывающемся списке **Изменить атрибут** выберите атрибут, который правило должно изменять:

      - **Отсутствует** – не изменять значения атрибутов. Значение 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 prepend** – 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.

5. Если вы хотите создать правило в карте маршрутизации, выполните следующие действия:

   a. Нажмите на кнопку **+ Правило**.

   b. Укажите параметры правила. Параметры правила описаны на шаге 4 этой инструкции.

   Правило будет создано. Вы можете добавить несколько правил и удалить правило, нажав рядом с ним на значок удаления ✕.

6. Нажмите на кнопку **Сохранить**.

   Карта маршрутизации будет изменена и обновится в таблице.

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

Удаление карты маршрутизации

Вы можете удалить карту маршрутизации в шаблоне CPE или на устройстве. Когда вы удаляете карту маршрутизации в шаблоне CPE, эта карта автоматически удаляется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Фильтры маршрутов → Карты маршрутизации**.

   - Если вы хотите удалить карту маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

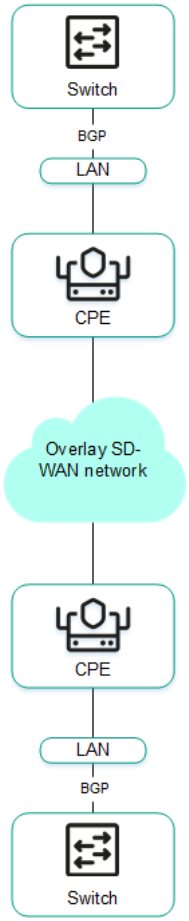
Обмен маршрутами по протоколу BGP

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).

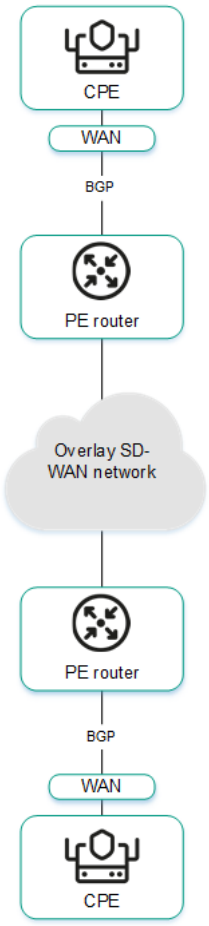
Поддерживается установка динамических TCP-сессий с группами BGP-соседей (англ. BGP peer groups), чтобы не создавать отдельных BGP-соседей (англ. BGP peers).

На рисунках ниже представлены примеры использования протокола динамической маршрутизации BGP в решении:

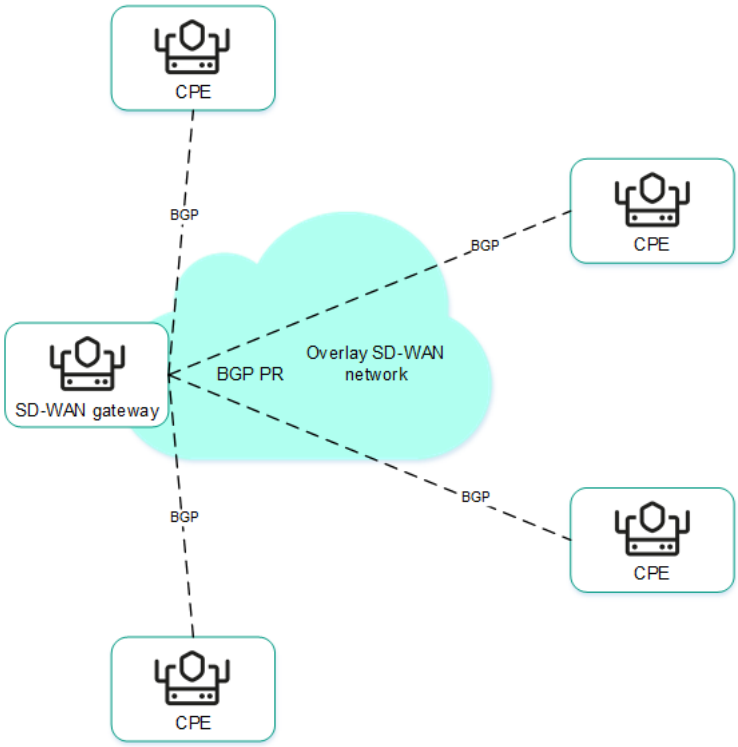
- Подключение нескольких клиентских площадок к сети L3 SD-WAN по BGP.



- 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. Когда вы указываете параметры BGP в шаблоне CPE, эти параметры автоматически распространяются на все использующие шаблон устройства.

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 и в отобразившейся области настройки выберите вкладку **Параметры BGP → Общие параметры**.

   - Если вы хотите настроить основные параметры BGP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры BGP → Общие параметры** и установите флажок **Переопределить**.

   Отобразятся основные параметры BGP.

2. В раскрывающемся списке **BGP** выберите **Включено**. По умолчанию выбрано значение **Выключено**.

3. Если вы хотите помещать BGP-маршруты на устройстве CPE в указанную виртуальную таблицу маршрутизации, в раскрывающемся списке **VRF** выберите ранее созданную виртуальную таблицу маршрутизации.

4. В поле **AS** введите номер автономной системы устройства CPE. Диапазон значений: от 1 до 4 294 967 295.

5. В поле **CPE 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:

   a. Установите флажок **Получить router ID из IP-пула**. По умолчанию флажок снят.

   b. В раскрывающемся списке **Пул IP** выберите ранее созданный диапазон IP-адресов.

6. При необходимости в поле **Лимит маршрутов** введите максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 8.

7. При необходимости установите следующие флажки:

   - Установите флажок **Всегда сравнивать MED**, чтобы устройство CPE сравнивало атрибут MED (multi-exit discriminator) маршрутов, анонсированных из разных автономных систем.

     Вам нужно убедиться, что этот 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**, чтобы включить перезагрузку Graceful restart на устройстве CPE.

   По умолчанию флажки сняты.

8. Если вы хотите, чтобы устройство CPE по умолчанию не обменивалось IPv4-маршрутами с BGP-соседями, снимите флажок **IPv4 unicast-маршруты по умолчанию**. По умолчанию флажок установлен.

9. Если вы хотите настроить BGP-таймеры, выполните следующие действия:

   a. Установите флажок **BGP-таймеры**. По умолчанию флажок снят.

   b. В поле **Keepalive** введите интервал в секундах для отправки устройством CPE контрольных пакетов BGP-соседям. Диапазон значений: от 0 до 65 535.

c. В поле **Holdtime** введите интервал 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.

10. 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 ранее созданную карту маршрутизации для перераспределяемых маршрутов.

    c. В поле **Метрика** введите метрику перераспределяемых маршрутов. Диапазон значений: от 0 до 16 777 214.

11. Если вы хотите, чтобы устройство CPE анонсировало BGP-соседям указанную сеть, 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 ранее созданную карту маршрутизации для подсети.

    Подсеть будет указана и отобразится в блоке **Сети**. Вы можете указать несколько подсетей и удалить подсеть, нажав рядом с ней на значок удаления ✕.

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

Работа с BGP-соседями (BGP peers)

Таблица BGP-соседей отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы BGP-соседей в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Параметры BGP → BGP-соседи**.
- Для отображения таблицы BGP-соседей на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Параметры BGP → 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** – унаследован ли BGP-сосед из шаблона CPE:
  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.
- **Удаленная AS** – номер автономной системы BGP-соседа.
- **Выключенный** – является ли BGP-сосед выключенным и установлена ли с ним TCP-сессия:
  - **Да** – BGP-сосед выключен и с ним не установлена TCP-сессия.
  - **Нет** – BGP-сосед включен и с ним установлена TCP-сессия.
- **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. Когда вы создаете BGP-соседа в шаблоне CPE, этот сосед автоматически создается на всех использующих шаблон устройствах. 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 и в отобразившейся области настройки выберите вкладку **Параметры BGP → BGP-соседи**.
   - Если вы хотите создать BGP-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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: 50 символов.
4. Если вы хотите выключить BGP-соседа и не устанавливать с ним TCP-сессию, установите флажок **Выключить BGP-соседа**. По умолчанию флажок снят.

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 успешного установления 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 **Loopback-интерфейс** введите IPv4-адрес loopback-интерфейса, который устройство CPE должно передавать 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**. По умолчанию флажок снят.

    b. В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE контрольных пакетов BGP-соседям. Диапазон значений: от 0 до 65 535.

    c. В поле **Holdtime** 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 считает его недоступным. Диапазон значений: от 0 до 65 535.

12. Если вы хотите использовать протокол BFD для обнаружения потери связности, установите флажок **BFD**. По умолчанию флажок снят.

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.

    - 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.

    - 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 этот 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 должно передавать 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**.

По умолчанию флажок снят.

g. Если вы хотите, чтобы устройство CPE анонсировало BGP-соседу маршрут по умолчанию 0.0.0.0/0, установите флажок **Маршрут по умолчанию**. По умолчанию флажок снят. Вы можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать ранее 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 ранее созданные карты маршрутизации, выполнив следующие действия:

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 ранее созданные списки префиксов, выполнив следующие действия:

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 ранее созданные списки управления доступом, выполнив следующие действия:

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

Изменение BGP-соседа

Вы можете изменить BGP-соседа в шаблоне CPE или на устройстве. Когда вы изменяете BGP-соседа в шаблоне CPE, этот сосед автоматически изменяется на всех использующих шаблон устройствах. Вы не можете изменить на устройстве CPE BGP-соседа, унаследованного из шаблона.

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 и в отобразившейся области настройки выберите вкладку **Параметры BGP → BGP-соседи**.

- Если вы хотите изменить BGP-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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 в поле **Имя** введите имя BGP-соседа. Максимальная длина: 50 символов.

4. Если вы хотите выключить BGP-соседа и не устанавливать с ним TCP-сессию, установите флажок **Выключить BGP-соседа**. По умолчанию флажок снят.

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 успешного установления 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 **Loopback-интерфейс** введите IPv4-адрес loopback-интерфейса, который устройство CPE должно передавать 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**. По умолчанию флажок снят.

    b. В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE контрольных пакетов BGP-соседям. Диапазон значений: от 0 до 65 535.

    c. В поле **Holdtime** 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 считает его недоступным. Диапазон значений: от 0 до 65 535.

12. Если вы хотите использовать протокол BFD для обнаружения потери связности, установите флажок **BFD**. По умолчанию флажок снят.

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.
    - 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.
    - 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 этот 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 должно передавать 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**.

По умолчанию флажок снят.

g. Если вы хотите, чтобы устройство CPE анонсировало BGP-соседу маршрут по умолчанию 0.0.0.0/0, установите флажок **Маршрут по умолчанию**. По умолчанию флажок снят. Вы можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать ранее 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 ранее созданные карты маршрутизации, выполнив следующие действия:

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 ранее созданные списки префиксов, выполнив следующие действия:

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 ранее созданные списки управления доступом, выполнив следующие действия:

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 **Сохранить**.

    BGP-сосед будет изменен и обновится в таблице.

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

Удаление BGP-соседа

Вы можете удалить BGP-соседа в шаблоне CPE или на устройстве. Когда вы удаляете BGP-соседа в шаблоне CPE, этот сосед автоматически удаляется на всех использующих шаблон устройствах. Вы не можете удалить на устройстве CPE BGP-соседа, унаследованного из шаблона.

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 и в отобразившейся области настройки выберите вкладку **Параметры BGP → BGP-соседи**.

   - Если вы хотите удалить BGP-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

Работа с группами BGP-соседей (BGP peer groups)

Таблица групп BGP-соседей отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы групп BGP-соседей в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Параметры BGP → Группы BGP-соседей**.

- Для отображения таблицы групп BGP-соседей на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство, в отобразившейся области настройки выбрать

вкладку **Параметры BGP** → **Группы BGP-соседей** и установить флажок **Переопределить**.

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** – унаследована ли группа BGP-соседей из шаблона CPE.
  - **Да**.
  - **Нет**.

  Этот столбец отображается только на устройстве CPE.
- **Удаленная AS** – номер автономной системы группы BGP-соседей.
- **Выключенный** – является ли группа BGP-соседей выключенной и установлена ли с ней TCP-сессия:
  - **Да** – группа BGP-соседей выключена и с ней не установлена TCP-сессия.
  - **Нет** – группа BGP-соседей включена и с ней установлена TCP-сессия.
- **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. Когда вы создаете группу BGP-соседей в шаблоне CPE, эта группа автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Параметры BGP** → **Группы BGP-соседей**.
   - Если вы хотите создать группу BGP-соседей на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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: 50 символов.

4. Если вы хотите выключить группу BGP-соседей и не устанавливать с ней TCP-сессию, установите флажок **Выключить группу BGP-соседей**. По умолчанию флажок снят.

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 успешного установления TCP-сессии между двумя BGP-соседями они должны использовать одинаковый пароль. Вы можете просмотреть введенный пароль, нажав на значок просмотра 👁.

9. В поле **Loopback-интерфейс** введите IPv4-адрес loopback-интерфейса, который устройство CPE должно передавать 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**. По умолчанию флажок снят.

    b. В поле **Keepalive** 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** 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 его недоступным. Диапазон значений: от 0 до 65 535.

12. Если вы хотите использовать протокол BFD для обнаружения потери связности, установите флажок **BFD**. По умолчанию флажок снят.

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.

    - 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.

    - 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 этот 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 должно передавать 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**.

По умолчанию флажок снят.

g. Если вы хотите, чтобы устройство CPE анонсировало группе BGP-соседей маршрут по умолчанию 0.0.0.0/0, установите флажок **Маршрут по умолчанию**. По умолчанию флажок снят. Вы можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать ранее 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 ранее созданные карты маршрутизации, выполнив следующие действия:

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 ранее созданные списки префиксов, выполнив следующие действия:

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 ранее созданные списки управления доступом, выполнив следующие действия:

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

Изменение группы BGP-соседей

Вы можете изменить группу BGP-соседей в шаблоне CPE или на устройстве. Когда вы изменяете группу BGP-соседей в шаблоне CPE, эта группа автоматически изменяется на всех использующих шаблон устройствах. Вы не можете изменить на устройстве CPE группу BGP-соседей, унаследованную из шаблона.

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 и в отобразившейся области настройки выберите вкладку **Параметры BGP → Группы BGP-соседей**.

- Если вы хотите изменить группу BGP-соседей на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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 в поле **Имя** введите имя группы BGP-соседей. Максимальная длина: 50 символов.

4. Если вы хотите выключить группу BGP-соседей и не устанавливать с ней TCP-сессию, установите флажок **Выключить группу BGP-соседей**. По умолчанию флажок снят.

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 успешного установления TCP-сессии между двумя BGP-соседями они должны использовать одинаковый пароль. Вы можете просмотреть введенный пароль, нажав на значок просмотра 👁.

9. В поле **Loopback-интерфейс** введите IPv4-адрес loopback-интерфейса, который устройство CPE должно передавать 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**. По умолчанию флажок снят.

    b. В поле **Keepalive** 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** 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 его недоступным. Диапазон значений: от 0 до 65 535.

12. Если вы хотите использовать протокол BFD для обнаружения потери связности, установите флажок **BFD**. По умолчанию флажок снят.

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.

    - 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.

    - 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 этот 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 должно передавать 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**.

По умолчанию флажок снят.

g. Если вы хотите, чтобы устройство CPE анонсировало группе BGP-соседей маршрут по умолчанию 0.0.0.0/0, установите флажок **Маршрут по умолчанию**. По умолчанию флажок снят. Вы можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать ранее 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 ранее созданные карты маршрутизации, выполнив следующие действия:

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 ранее созданные списки префиксов, выполнив следующие действия:

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 ранее созданные списки управления доступом, выполнив следующие действия:

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 **Сохранить**.

    Группа BGP-соседей будет изменена и обновится в таблице.

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

Удаление группы BGP-соседей

Вы можете удалить группу BGP-соседей в шаблоне CPE или на устройстве. Когда вы удаляете группу BGP-соседей в шаблоне CPE, эта группа автоматически удаляется на всех использующих шаблон устройствах. Вы не можете удалить на устройстве CPE группу BGP-соседей, унаследованную из шаблона.

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 и в отобразившейся области настройки выберите вкладку **Параметры BGP** → **Группы BGP-соседей**.

   - Если вы хотите удалить группу BGP-соседей на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

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 вы можете создавать OSPF-области (англ. OSPF areas) и OSPF-интерфейсы.

Настройка основных параметров OSPF

Вы можете настроить основные параметры OSPF в шаблоне CPE или на устройстве. Когда вы указываете параметры OSPF в шаблоне CPE, эти параметры автоматически распространяются на все использующие шаблон устройства.

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 и в отобразившейся области настройки выберите вкладку **OSPF → Общие параметры**.

   - Если вы хотите настроить основные параметры OSPF на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **OSPF → Общие параметры** и установите флажок **Переопределить**.

   Отобразятся параметры OSPF.

2. В раскрывающемся списке **OSPF** выберите **Включено**. По умолчанию выбрано значение **Выключено**.

3. В поле **CPE 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 каналов 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 **Пассивные интерфейсы по умолчанию**. В пассивном режиме OSPF-интерфейсы не обмениваются

пакетами трафика. По умолчанию флажок снят.

8. Если вы хотите вести журнал OSPF, установите флажок **Журнал изменений смежности**. Вы можете установить флажок **Журнал изменений смежности**, 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 ранее 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 ранее созданный список управления доступом для перераспределяемых маршрутов. По умолчанию флажок снят.

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**. По умолчанию флажок снят.

    b. Установите флажок **Применять всегда**, чтобы всегда анонсировать маршрут по умолчанию 0.0.0.0/0, даже если он отсутствует в таблице маршрутизации устройства CPE. По умолчанию флажок снят.

    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 ранее 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**. По умолчанию флажок снят.

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 областей одного OSPF-домена. Диапазон значений: от 1 до 255.

d. В поле **Внутри области** введите административную дистанцию для маршрутов из одной 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**. По умолчанию флажок снят.

b. В поле **Длительность Grace period (сек.)** введите время в секундах, в течение которого устройство CPE должно анонсировать 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**. По умолчанию флажок снят.

b. В поле **Задержка (сек.)** введите время задержки в секундах перед началом вычислений SPF-алгоритма. Диапазон значений: от 0 до 600 000.

c. В поле **Изначальное время удержания (мсек.)** введите минимальное время удержания в миллисекундах между двумя вычислениями SPF-алгоритма. Диапазон значений: от 0 до 600 000.

d. В поле **Максимальное время удержания (мсек.)** 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 канала (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 канала OSPF-соседям.

b. Если вы хотите указать время, в течение которого устройство CPE должно использовать максимальную метрику в анонсах состояния канала OSPF-соседям при запуске или перезапуске

протокола OSPF, выполните следующие действия:

1. Установите флажок **При запуске**. По умолчанию флажок снят.
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 должно использовать максимальную метрику в анонсах состояния канала OSPF-соседям при выключении протокола OSPF, выполните следующие действия:

1. Установите флажок **При выключении**. По умолчанию флажок снят.
2. В поле **Таймер (сек.)** введите время в секундах. Диапазон значений: от 5 до 100.

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

Работа с OSPF-областями

Таблица OSPF-областей отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы OSPF-областей в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **OSPF → OSPF-области**.
- Для отображения таблицы OSPF-областей на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки 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. Когда вы создаете OSPF-область в шаблоне CPE, эта область автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **OSPF → OSPF-области**.

   - Если вы хотите создать OSPF-область на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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**. По умолчанию флажок снят.

   b. В раскрывающемся списке **Тип области** выберите тип тупиковой 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**. По умолчанию флажок снят.

   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**. По умолчанию флажок снят.

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 должно выполняться с маршрутами:

- **Анонсировать** – анонсировать маршруты по протоколу OSPF. Значение 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 диапазон, нажав рядом с ним на значок удаления ✕.

8. Если вы хотите соединить OSPF-область с другой областью через транзитную область, укажите виртуальный канал, выполнив следующие действия:

   a. В блоке **Виртуальные соединения** нажмите на кнопку **+ Виртуальное соединение**.

   b. В поле **Адрес** введите IPv4-адрес сетевого интерфейса маршрутизатора в транзитной области.

   Виртуальный канал будет указан и отобразится в блоке **OSPF-диапазоны**. Вы можете указать несколько виртуальных каналов и удалить канал, нажав рядом с ним на значок удаления ✕.

9. Если вы хотите настроить фильтрацию маршрутов для OSPF-области, в блоке **Фильтрация** выполните следующие действия:

   a. Выберите ранее созданные списки управления доступом, выполнив следующие действия:

      1. В раскрывающемся списке **Список экспорта** выберите список управления доступом для маршрутов, которые анонсируются из OSPF-области в другие области.
      2. В раскрывающемся списке **Список импорта** выберите список управления доступом для маршрутов, которые анонсируются из других OSPF-областей в область.

   b. Выберите ранее созданные списки префиксов, выполнив следующие действия:

      1. В раскрывающемся списке **Исходящий список фильтрации** выберите список префиксов для маршрутов, которые анонсируются из OSPF-области в другие области.
      2. В раскрывающемся списке **Входящий список фильтрации** выберите список префиксов для маршрутов, которые анонсируются из других OSPF-областей в область.

10. Нажмите на кнопку **Сохранить**.

    OSPF-область будет создана и отобразится в таблице.

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

Изменение OSPF-области

Вы можете изменить OSPF-область в шаблоне CPE или на устройстве. Когда вы изменяете OSPF-область в шаблоне CPE, эта область автоматически изменяется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **OSPF → OSPF-области**.

   - Если вы хотите изменить OSPF-область на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 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**. По умолчанию флажок снят.

   b. В раскрывающемся списке **Тип области** выберите тип тупиковой 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**. По умолчанию флажок снят.

   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**. По умолчанию флажок снят.

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 должно выполняться с маршрутами:

- **Анонсировать** – анонсировать маршруты по протоколу OSPF. Значение 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 диапазон, нажав рядом с ним на значок удаления ✕.

8. Если вы хотите соединить OSPF-область с другой областью через транзитную область, укажите виртуальный канал, выполнив следующие действия:

   a. В блоке **Виртуальные соединения** нажмите на кнопку **+ Виртуальное соединение**.

   b. В поле **Адрес** введите IPv4-адрес сетевого интерфейса маршрутизатора в транзитной области.

   Виртуальный канал будет указан и отобразится в блоке **OSPF-диапазоны**. Вы можете указать несколько виртуальных каналов и удалить канал, нажав рядом с ним на значок удаления ✕.

9. Если вы хотите настроить фильтрацию маршрутов для OSPF-области, в блоке **Фильтрация** выполните следующие действия:

   a. Выберите ранее созданные списки управления доступом, выполнив следующие действия:

      1. В раскрывающемся списке **Список экспорта** выберите список управления доступом для маршрутов, которые анонсируются из OSPF-области в другие области.
      2. В раскрывающемся списке **Список импорта** выберите список управления доступом для маршрутов, которые анонсируются из других OSPF-областей в область.

   b. Выберите ранее созданные списки префиксов, выполнив следующие действия:

      1. В раскрывающемся списке **Исходящий список фильтрации** выберите список префиксов для маршрутов, которые анонсируются из OSPF-области в другие области.
      2. В раскрывающемся списке **Входящий список фильтрации** выберите список префиксов для маршрутов, которые анонсируются из других OSPF-областей в область.

10. Нажмите на кнопку **Сохранить**.

    OSPF-область будет изменена и обновится в таблице.

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

Удаление OSPF-области

Вы можете удалить OSPF-область в шаблоне CPE или на устройстве. Когда вы удаляете OSPF-область в шаблоне CPE, эта область автоматически удаляется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **OSPF** → **OSPF-области**.

   - Если вы хотите удалить OSPF-область на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

Работа с OSPF-интерфейсами

Таблица OSPF-интерфейсов отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы OSPF-интерфейсов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **OSPF** → **OSPF-интерфейсы**.

- Для отображения таблицы OSPF-интерфейсов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **Устройства CPE**, нажать на устройство и в отобразившейся области настройки 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. Когда вы создаете OSPF-интерфейс в шаблоне CPE, этот интерфейс автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **OSPF** → **OSPF-интерфейсы**.

   - Если вы хотите создать OSPF-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 ранее 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**. По умолчанию флажок снят.

11. Если вы хотите настроить OSPF-таймеры, выполните следующие действия:

    a. Установите флажок **OSPF-таймеры**. По умолчанию флажок снят.

    b. В поле **Hello-интервал (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-интервал (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 его недоступным. Диапазон значений: от 1 до 65 535.

12. В поле **Интервал повторной передачи (сек.)** введите интервал времени в секундах для повторной отправки OSPF-интерфейсом потерянных пакетов трафика. Диапазон значений от 1 до 65 535.

13. В поле **Задержка при передаче (сек.)** введите время задержки в секундах перед отправкой OSPF-интерфейсом первого пакета трафика. Диапазон значений от 1 до 65 535.

14. Нажмите на кнопку **Создать**.

    OSPF-интерфейс будет создан и отобразится в таблице.

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

Изменение OSPF-интерфейса

Вы можете изменить OSPF-интерфейс в шаблоне CPE или на устройстве. Когда вы изменяете OSPF-интерфейс в шаблоне CPE, этот интерфейс автоматически изменяется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **OSPF → OSPF-интерфейсы**.

   - Если вы хотите изменить OSPF-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 в раскрывающемся списке **Интерфейс** выберите ранее 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**. По умолчанию флажок снят.

11. Если вы хотите настроить OSPF-таймеры, выполните следующие действия:

a. Установите флажок **OSPF-таймеры**. По умолчанию флажок снят.

b. В поле **Hello-интервал (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-интервал (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 его недоступным. Диапазон значений: от 1 до 65 535.

12. В поле **Интервал повторной передачи (сек.)** введите интервал времени в секундах для повторной отправки OSPF-интерфейсом потерянных пакетов трафика. Диапазон значений от 1 до 65 535.

13. В поле **Задержка при передаче (сек.)** введите время задержки в секундах перед отправкой OSPF-интерфейсом первого пакета трафика. Диапазон значений от 1 до 65 535.

14. Нажмите на кнопку **Сохранить**.

    OSPF-интерфейс будет изменен и обновится в таблице.

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

Удаление OSPF-интерфейса

Вы можете удалить OSPF-интерфейс в шаблоне CPE или на устройстве. Когда вы удаляете OSPF-интерфейс в шаблоне CPE, этот интерфейс автоматически удаляется на всех использующих шаблон устройствах.

> 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 и в отобразившейся области настройки выберите вкладку **OSPF** → **OSPF-интерфейсы**.

   - Если вы хотите удалить OSPF-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

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 каналах и туннелях. 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.

Таблица BFD-соседей отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы BFD-соседей в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Параметры BFD**.
- Для отображения таблицы BFD-соседей на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство, в отобразившейся области настройки выбрать вкладку **Параметры BFD**.

Информация о BFD-соседях отображается в следующих столбцах таблицы:

- **Имя** – имя BFD-соседа
- **IP-адрес** – IPv4-адрес BFD-соседа.
- **Интервал передачи (мсек.)** – интервал в миллисекундах для отправки устройством CPE контрольных пакетов BFD-соседу.
- **Интервал получения (мсек.)** – интервал 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 его 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 должно ожидать получения контрольных пакетов от BFD-соседа. Если в течение этого времени от BFD-соседа не поступает контрольных пакетов, устройство 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. Когда вы включаете или выключаете протокол BFD в шаблоне CPE, этот протокол автоматически включается или выключается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Параметры BFD**.

- Если вы хотите включить или выключить протокол BFD на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры BFD** и установите флажок **Переопределить**.

Отобразится таблица BFD-соседей.

2. В раскрывающемся списке **BFD** выберите одно из следующих значений:

   - **Включено**.

   - **Выключено** – значение по умолчанию.

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

Создание BFD-соседа

Вы можете создать BFD-соседа в шаблоне CPE или на устройстве. Когда вы создаете BFD-соседа в шаблоне CPE, этот сосед автоматически создается на всех использующих шаблон устройствах. 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 и в отобразившейся области настройки выберите вкладку **Параметры BFD**.

   - Если вы хотите создать BFD-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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: 255 символов.

4. В поле **IP-адрес** введите IPv4-адрес BFD-соседа.

5. В поле **Интервал передачи (мсек.)** введите интервал времени в миллисекундах для отправки устройством CPE контрольных пакетов BFD-соседу. Диапазон значений: от 60 до 10000.

6. В поле **Интервал получения (мсек.)** 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 его 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 должно ожидать получения контрольных пакетов от BFD-соседа. Если в течение этого времени от BFD-соседа не поступает контрольных пакетов, устройство 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 условии, что устройство не получило ни одного контрольного пакета от BFD-соседа.

8. Нажмите на кнопку **Создать**.

   BFD-сосед будет создан и отобразится в таблице.

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

Изменение BFD-соседа

Вы можете изменить BFD-соседа в шаблоне CPE или на устройстве. Когда вы изменяете BFD-соседа в шаблоне CPE, этот BFD-сосед автоматически изменяется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Параметры BFD**.

   - Если вы хотите изменить BFD-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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 в поле **Имя** введите имя BFD-соседа. Максимальная длина: 255 символов.

4. В поле **IP-адрес** введите IPv4-адрес BFD-соседа.

5. В поле **Интервал передачи (мсек.)** введите интервал времени в миллисекундах для отправки устройством CPE контрольных пакетов BFD-соседу. Диапазон значений: от 60 до 10000.

6. В поле **Интервал получения (мсек.)** 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 его 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 должно ожидать получения контрольных пакетов от BFD-соседа. Если в течение этого времени от BFD-соседа не поступает контрольных пакетов, устройство 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 условии, что устройство не получило ни одного контрольного пакета от BFD-соседа.

8. Нажмите на кнопку **Сохранить**.

   BFD-сосед будет изменен и обновится в таблице.

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

Удаление BFD-соседа

Вы можете удалить BFD-соседа в шаблоне CPE или на устройстве. Когда вы удаляете BFD-соседа в шаблоне CPE, этот сосед автоматически удаляется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Параметры BFD**.
   - Если вы хотите удалить BFD-соседа на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

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, и виртуальный IP-адрес назначается ему. 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 выбрать сетевой интерфейс, а также указать 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 в группе, это изменение происходит в остальных экземплярах в группе.

Включение и выключение протокола VRRP

Вы можете включить или выключить протокол VRRP в шаблоне CPE или на устройстве. Когда вы включаете или выключаете протокол VRRP в шаблоне CPE, этот протокол автоматически включается или выключается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **VRRP → Экземпляры VRRP**.

   - Если вы хотите включить или выключить протокол VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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** – значение по умолчанию.

   При включении протокола VRRP вам нужно создать хотя бы один экземпляр VRRP.

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

Работа с экземплярами VRRP

Таблица экземпляров VRRP отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы экземпляров VRRP в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **VRRP → Экземпляры VRRP**.

- Для отображения таблицы экземпляров VRRP на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство, в отобразившейся области настройки 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, добавленный 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 в секундах для отправки сетевым интерфейсом контрольных пакетов другим сетевым интерфейсам.
- **Оставлять резервным при восстановлении** – должна ли измениться роль сетевого интерфейса, ставшего основным, 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. Когда вы создаете экземпляр VRRP в шаблоне CPE, этот экземпляр автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **VRRP → Экземпляры VRRP**.

- Если вы хотите создать экземпляр VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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: 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 ранее 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. Значение 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 1000. По умолчанию указано значение `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. По умолчанию указано значение `5`.

10. При необходимости не изменять роль резервного сетевого интерфейса, ставшего основным, если прежний основной сетевой интерфейс восстанавливает работу, установите флажок **Оставлять резервным при восстановлении**. По умолчанию флажок снят.

11. Если вы хотите настроить unicast-отправку контрольных пакетов сетевым интерфейсом, выполните следующие действия:

    a. Установите флажок **Unicast**. По умолчанию флажок снят.

    b. В поле **IP основного VRRP-маршрутизатора** введите IP-адрес сетевого интерфейса, с которого вы хотите отправлять контрольные пакеты.

    c. В поле **IP резервного VRRP-маршрутизатора** введите IP-адрес сетевого интерфейса, на который вы хотите отправлять контрольные пакеты.

    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**. По умолчанию флажок снят.

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

Изменение экземпляра VRRP

Вы можете изменить экземпляр VRRP в шаблоне CPE или на устройстве. Когда вы изменяете экземпляр VRRP в шаблоне CPE, этот экземпляр автоматически изменяется на всех использующих шаблон устройствах. Вы не можете изменить на устройстве CPE экземпляр VRRP, унаследованный из шаблона.

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 и в отобразившейся области настройки выберите вкладку **VRRP** → **Экземпляры VRRP**.

   - Если вы хотите изменить экземпляр VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **VRRP** → **Экземпляры VRRP** и в верхней части области настройки установите флажок **Переопределить**.

   Отобразится таблица экземпляров VRPP.

2. Нажмите на кнопку **Изменить** рядом с экземпляром VRRP, который вы хотите изменить.

3. В открывшемся окне в поле **Имя** введите имя экземпляра VRRP. Максимальная длина: 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 ранее 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. Значение 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 1000. По умолчанию указано значение `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. По умолчанию указано значение `5`.

10. При необходимости не изменять роль резервного сетевого интерфейса, ставшего основным, если прежний основной сетевой интерфейс восстанавливает работу, установите флажок **Оставлять резервным при восстановлении**. По умолчанию флажок снят.

11. Если вы хотите настроить unicast-отправку контрольных пакетов сетевым интерфейсом, выполните следующие действия:

    a. Установите флажок **Unicast**. По умолчанию флажок снят.

    b. В поле **IP основного VRRP-маршрутизатора** введите IP-адрес сетевого интерфейса, с которого вы хотите отправлять контрольные пакеты.

    c. В поле **IP резервного VRRP-маршрутизатора** введите IP-адрес сетевого интерфейса, на который вы хотите отправлять контрольные пакеты.

    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**. По умолчанию флажок снят.

    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 **Сохранить**.

    Экземпляр VRRP будет изменен и обновится в таблице.

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

Удаление экземпляра VRRP

Вы можете удалить экземпляр VRRP в шаблоне CPE или на устройстве. Когда вы удаляете экземпляр VRRP в шаблоне CPE, этот экземпляр автоматически удаляется на всех использующих шаблон устройствах. Вы не можете удалить на устройстве CPE экземпляр VRRP, унаследованный из шаблона.

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 и в отобразившейся области настройки выберите вкладку **VRRP** → **Экземпляры VRRP**.

   - Если вы хотите удалить экземпляр VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

Работа с группами экземпляров VRRP

Таблица групп экземпляров VRRP отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы групп экземпляров VRRP в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **VRRP** → **Группы экземпляров VRRP**.

- Для отображения таблицы групп экземпляров VRRP на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **Устройства CPE**, нажать на устройство и в отобразившейся области настройки 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, добавленные в группу.

- **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. Когда вы создаете группу экземпляров VRRP в шаблоне CPE, эта группа автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **VRRP → Группы экземпляров VRRP**.

- Если вы хотите создать группу экземпляров VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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: 16 символов. По умолчанию указано значение `1`.

4. В раскрывающемся списке **Экземпляры VRRP** выберите ранее созданные экземпляры VRRP, которые вы хотите добавить в группу.

5. Нажмите на кнопку **Создать**.

   Группа экземпляров VRRP будет создана и отобразится в таблице.

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

Изменение группы экземпляров VRRP

Вы можете изменить группу экземпляров VRRP в шаблоне CPE или на устройстве. Когда вы изменяете группу экземпляров VRRP в шаблоне CPE, эта группа автоматически изменяется на всех использующих шаблон устройствах. Вы не можете изменить на устройстве CPE группу экземпляров VRRP, унаследованную из шаблона.

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 и в отобразившейся области настройки выберите вкладку **VRRP → Группы экземпляров VRRP**.

   - Если вы хотите изменить группу экземпляров VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 в поле **Имя** введите имя группы экземпляров VRRP. Максимальная длина: 16 символов. По умолчанию указано значение `1`.

4. В раскрывающемся списке **Экземпляры VRRP** выберите ранее созданные экземпляры VRRP, которые вы хотите добавить в группу.

5. Нажмите на кнопку **Сохранить**.

Группа экземпляров VRRP будет изменена и обновится в таблице.

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

Удаление группы экземпляров VRRP

Вы можете удалить группу экземпляров VRRP в шаблоне CPE или на устройстве. Когда вы удаляете группу экземпляров VRRP в шаблоне CPE, эта группа автоматически удаляется на всех использующих шаблон устройствах. Вы не можете удалить на устройстве CPE группу экземпляров VRRP, унаследованную из шаблона.

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 и в отобразившейся области настройки выберите вкладку **VRRP → Группы экземпляров VRRP**.

   - Если вы хотите удалить группу экземпляров VRRP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

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. В качестве multicast-интерфейсов используются ранее 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. Запросы содержат IP-адреса источников, от которых клиенты хотят получать пакеты multicast-трафика. Когда источники отправляют пакеты multicast-трафика на точку рандеву, клиенты получают эти пакеты.

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. Когда вы указываете параметры PIM в шаблоне CPE, эти параметры автоматически распространяются на все использующие шаблон устройства.

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 и в отобразившейся области настройки выберите вкладку **Multicast → Общие параметры**.

   - Если вы хотите настроить основные параметры PIM на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **Multicast → Общие параметры**.

   Отобразятся основные параметры PIM.

2. В раскрывающемся списке **Multicast** выберите **Включено**. По умолчанию выбрано значение **Выключено**.

3. Укажите точку рандеву для источников пакетов multicast-трафика и подключенных к устройству CPE клиентов, выполнив следующие действия:

   a. В блоке **RP IP** нажмите на кнопку **+ Добавить**.

   b. В отобразившемся поле введите IPv4-адрес точки рандеву.

   c. 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 точку, нажав 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. По умолчанию указано значение `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 ранее созданный список префиксов.

6. Если устройство CPE находится на последнем хопе, и вы хотите запретить на этом устройстве 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**. По умолчанию флажок снят.

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 ранее 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**. По умолчанию флажок снят. Для выполнения ECMP-балансировки требуется наличие нескольких маршрутов. Если ECMP-балансировка выключена, трафик передается по одному маршруту.

   b. При необходимости перераспределить весь трафик между оставшимися маршрутами, если один из multicast-интерфейсов выходит из строя, установите флажок **Перебалансировка ECMP**. По умолчанию флажок снят, и при выходе из строя одного из multicast-интерфейсов перераспределяются только трафик, передававшийся через этот multicast-интерфейс.

8. В поле **Интервал присоединения/отказа PIM** введите интервал в секундах для отправки multicast-интерфейсами пакетов join/prune PIM-соседям. Диапазон значений: от 60 до 600. По умолчанию указано значение `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. По умолчанию указано значение `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 ранее 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** – значение по умолчанию.
    - **urib-only**.

12. Если вы хотите добавить в таблицу multicast-маршрутизации устройства CPE статический IPv4-маршрут, выполните следующие действия:

    a. В блоке **Статический multicast-маршрут** 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** – ранее 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 **Статический multicast-маршрут**. Вы можете добавить несколько статических маршрутов и удалить маршрут, нажав рядом с ним на значок удаления ✕.

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

Работа с multicast-интерфейсами

Таблица multicast-интерфейсов отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы multicast-интерфейсов в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Multicast → Интерфейсы**.

- Для отображения таблицы multicast-интерфейсов на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Multicast → Интерфейсы**.

Информация о multicast-интерфейсах отображается в следующих столбцах таблицы:

- **Сетевой интерфейс** – сетевой интерфейс, который используется как multicast-интерфейс.

- **PIM** – включен ли на multicast-интерфейсе обмен сообщениями по протоколу PIM с соседями:

  - **Включено**.

  - **Выключено**.

- **IGMP** – включен ли на multicast-интерфейсе 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** – унаследован ли multicast-интерфейс 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. Когда вы создаете multicast-интерфейс в шаблоне CPE, этот интерфейс автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Multicast → Интерфейсы**.

   - Если вы хотите создать multicast-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 ранее созданный сетевой интерфейс, который вы хотите использовать как multicast-интерфейс.

4. Настройте протокол PIM на multicast-интерфейсе, выполнив следующие действия:

   a. В раскрывающемся списке **PIM** выберите **Включено**. По умолчанию выбрано значение **Выключено**.

   b. Если вы хотите перевести multicast-интерфейс в пассивный режим, установите флажок **Пассивный**. В пассивном режиме multicast-интерфейсы не обмениваются контрольными пакетами. По умолчанию флажок снят.

   c. Если вы хотите запретить обмен bootstrap-пакетами на multicast-интерфейсе, снимите флажок **BSM**. По умолчанию флажок установлен.

   d. Если вы хотите запретить обмен unicast bootstrap-пакетами на multicast-интерфейсе, снимите флажок **Unicast BSM**. По умолчанию флажок установлен.

   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. По умолчанию указано значение `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. По умолчанию указано значение `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 соседа не поступает

контрольных пакетов, multicast-интерфейс считает его недоступным. Диапазон значений: от 1 до 630. По умолчанию указано значение `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, выполнив следующие действия:

a. В раскрывающемся списке **IGMP** выберите **Включено**. По умолчанию выбрано значение **Выключено**.

b. В раскрывающемся списке **Версия** выберите версию протокола IGMP на multicast-интерфейсе:

- **2**.
- **3** – значение 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. По умолчанию указано значение `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. По умолчанию указано значение `10`.

e. Если вы хотите указать multicast-группы, выполните следующие действия:

1. В блоке**Группа присоединения** нажмите на кнопку **+ Добавить**.
2. В отобразившемся поле введите IPv4-адрес multicast-группы.
3. 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 группу, нажав 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 этот сегмент требуется отправлять пакеты трафика от multicast-группы.

6. Нажмите на кнопку **Сохранить**.

Multicast-интерфейс будет создан и отобразится в таблице.

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

Изменение multicast-интерфейса

Вы можете изменить параметры multicast-интерфейса в шаблоне CPE или на устройстве. Когда вы изменяете multicast-интерфейс в шаблоне CPE, этот интерфейс автоматически изменяется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Multicast** → **Интерфейсы**.

   - Если вы хотите изменить multicast-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 в раскрывающемся списке **Сетевой интерфейс** выберите ранее созданный сетевой интерфейс, который вы хотите использовать как multicast-интерфейс.

4. Настройте протокол PIM на multicast-интерфейсе, выполнив следующие действия:

   a. В раскрывающемся списке **PIM** выберите **Включено**. По умолчанию выбрано значение **Выключено**.

   b. Если вы хотите перевести multicast-интерфейс в пассивный режим, установите флажок **Пассивный**. В пассивном режиме multicast-интерфейсы не обмениваются контрольными пакетами. По умолчанию флажок снят.

   c. Если вы хотите запретить обмен bootstrap-пакетами на multicast-интерфейсе, снимите флажок **BSM**. По умолчанию флажок установлен.

   d. Если вы хотите запретить обмен unicast bootstrap-пакетами на multicast-интерфейсе, снимите флажок **Unicast BSM**. По умолчанию флажок установлен.

   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. По умолчанию указано значение `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. По умолчанию указано значение `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 соседа не поступает контрольных пакетов, multicast-интерфейс считает его недоступным. Диапазон значений: от 1 до 630. По умолчанию указано значение `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, выполнив следующие действия:

   a. В раскрывающемся списке **IGMP** выберите **Включено**. По умолчанию выбрано значение **Выключено**.

b. В раскрывающемся списке **Версия** выберите версию протокола IGMP на multicast-интерфейсе:

- **2**.
- **3** – значение 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. По умолчанию указано значение `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. По умолчанию указано значение `10`.

e. Если вы хотите указать multicast-группы, выполните следующие действия:

1. В блоке**Группа присоединения** нажмите на кнопку **+ Добавить**.
2. В отобразившемся поле введите IPv4-адрес multicast-группы.
3. 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 группу, нажав 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 этот сегмент требуется отправлять пакеты трафика от multicast-группы.

6. Нажмите на кнопку **Сохранить**.

   Multicast-интерфейс будет изменен и обновится в таблице.

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

Удаление multicast-интерфейса

Вы можете удалить multicast-интерфейс в шаблоне CPE или на устройстве. Когда вы удаляете multicast-интерфейс в шаблоне CPE, этот интерфейс автоматически удаляется на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **Multicast** → **Интерфейсы**.

- Если вы хотите удалить multicast-интерфейс на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

Работа с виртуальными таблицами маршрутизации (VRF)

Kaspersky SD-WAN поддерживает технологию Virtual Routing and Forwarding (VRF) для создания до 200 виртуальных таблиц маршрутизации на устройствах CPE.

При создании виртуальной таблицы маршрутизации вы выбираете сетевые интерфейсы, которые хотите в нее добавить. Сетевые интерфейсы для подключения устройства CPE к контроллеру и оркестратору автоматически добавляются в виртуальную таблицу маршрутизацию по умолчанию, и вы не можете добавить их в другие таблицы. Один сетевой интерфейс невозможно добавить в несколько виртуальных таблиц маршрутизации.

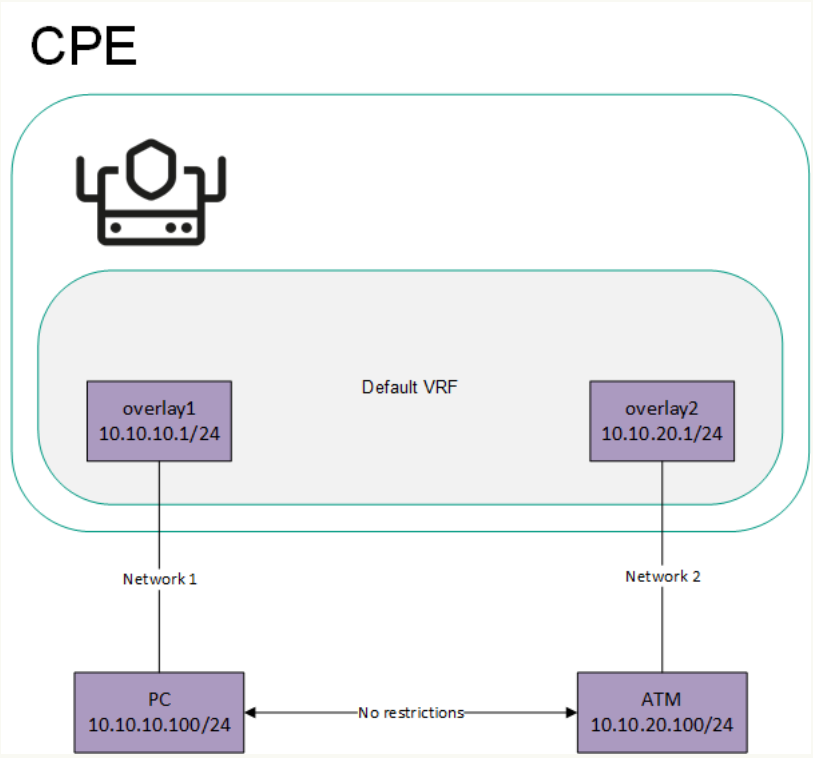
Если два сетевых интерфейса находятся в разных виртуальных таблицах маршрутизации, подключенные к ним сети не имеют доступа друг к другу. При этом сетевым интерфейсам могут быть назначены IP-адреса из одинаковых или пересекающихся подсетей.

Вы можете поместить в виртуальные таблицы маршрутизации BGP-маршруты и статические маршруты. Для помещения BGP-маршрутов в виртуальную таблицу вам нужно указать эту таблицу при настройке основных параметров BGP. Для помещения статического маршрута в виртуальную таблицу маршрутизации вам нужно указать эту таблицу при создании или изменении статического маршрута.

Виртуальные таблицы маршрутизации можно использовать в следующих сценариях:

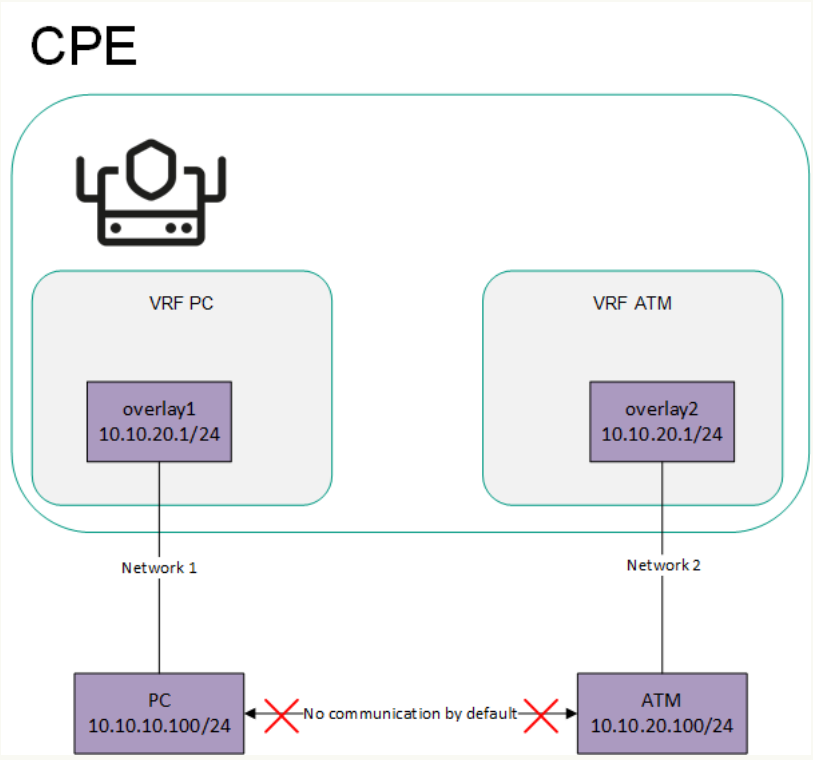
- **Сегментация сети с помощью виртуальных таблиц маршрутизации**.

Вы можете создать виртуальные таблицы маршрутизации, чтобы сегментировать сеть. На рисунке ниже сеть Network 1 построена между сетевым интерфейсом overlay1 и пользовательским персональными компьютерами (PC), а Network 2 – между сетевым интерфейсом overlay2 и банкоматами (ATM). Оба сетевых интерфейса находятся в виртуальной таблице маршрутизации по умолчанию (Default VRF), 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 Network 1 и Network 2 сетевые интерфейсы overlay1 и overlay2 необходимо добавить в отдельные виртуальные таблицы маршрутизации, в результате чего будут созданы два сегмента (см. рисунок ниже).

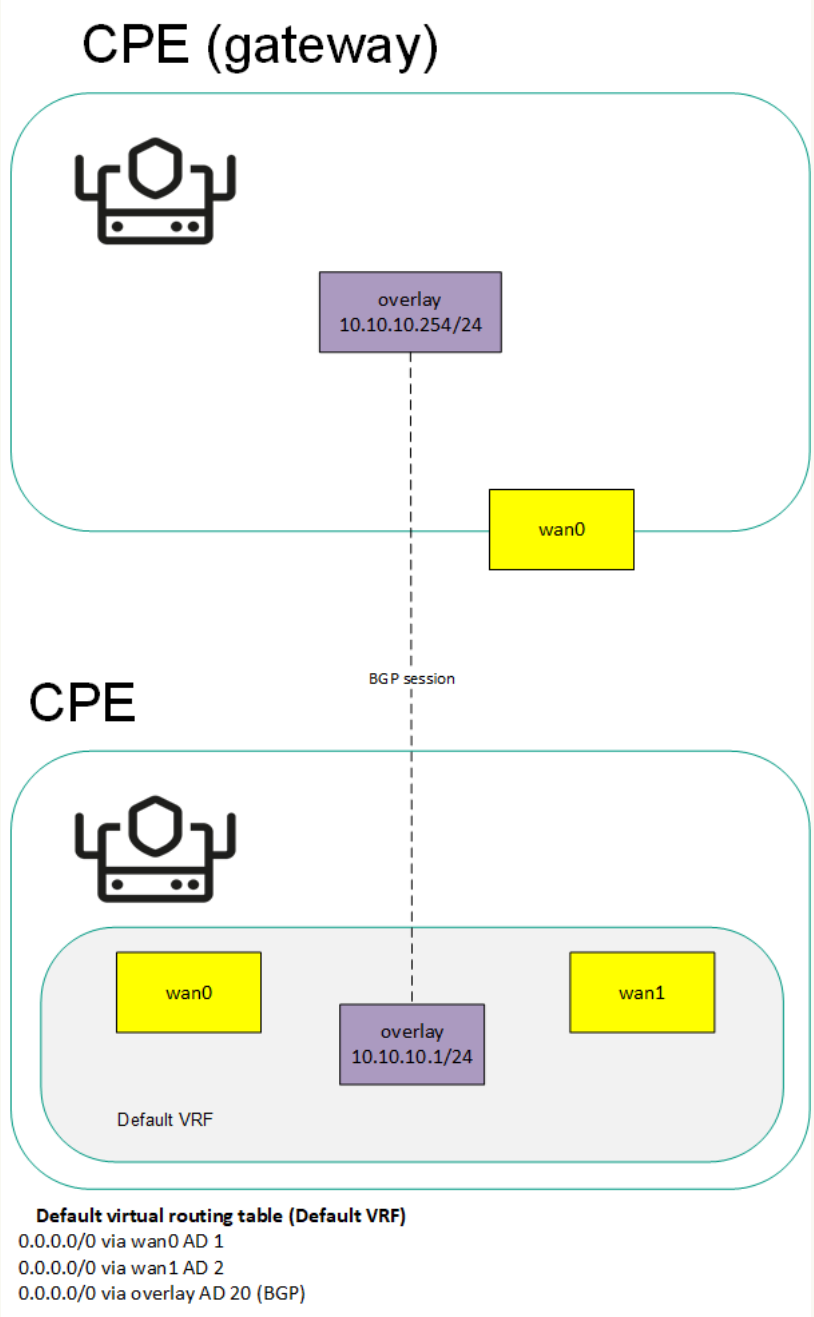


Подключенные к разным сетям сетевые интерфейсы в отдельных виртуальных таблицах маршрутизации

- Передача маршрута 0.0.0.0/0 по протоколу BGP.

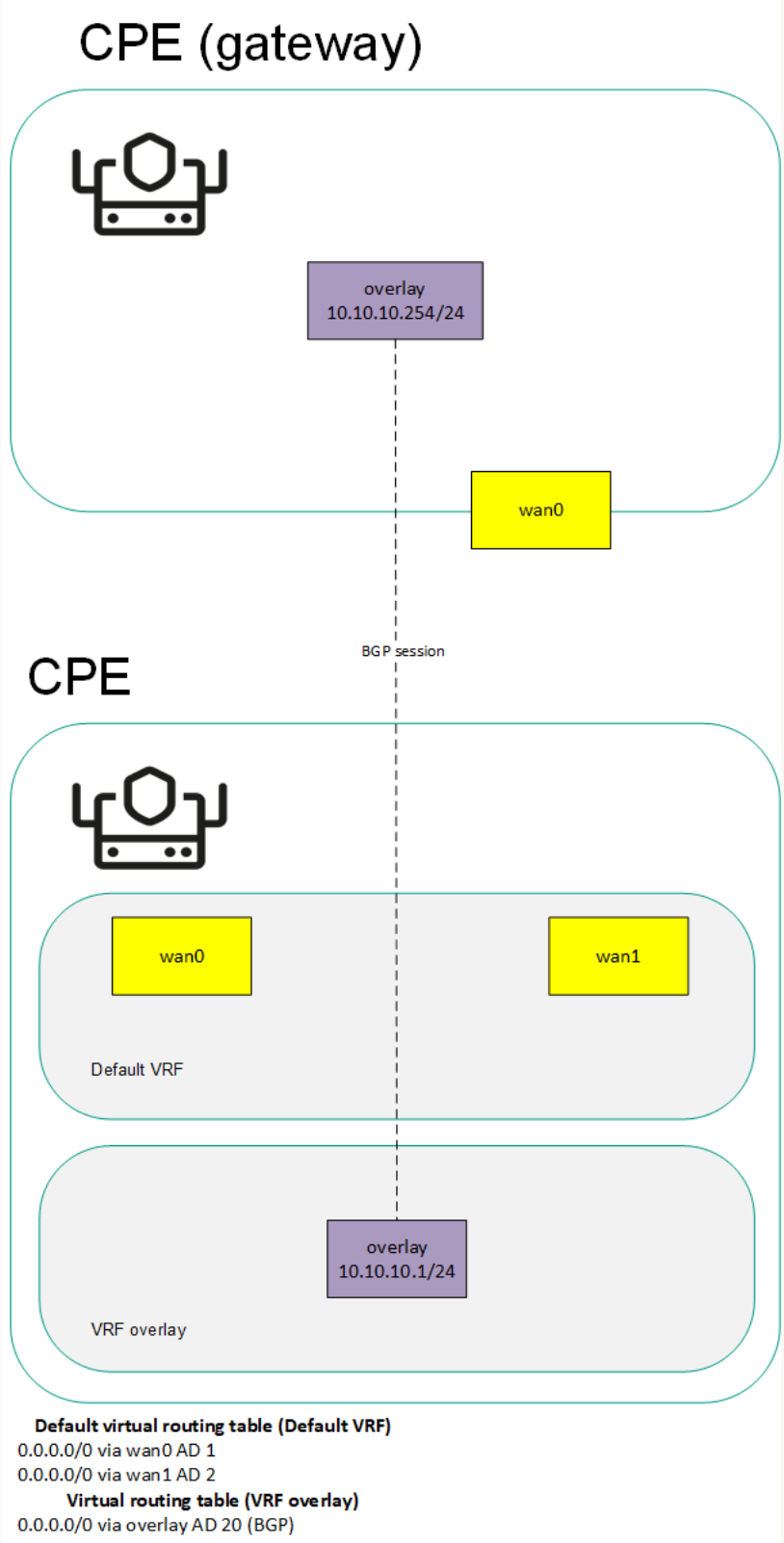
Вы можете создать отдельную виртуальную таблицу маршрутизации, чтобы передавать между устройствами маршрут 0.0.0.0/0 по протоколу BGP. На рисунке ниже представлено устройство CPE с ролью шлюз (GW) и стандартное устройство. Все устройства CPE добавлены в виртуальную таблицу маршрутизации по умолчанию.

Если шлюз 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, этот 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 таблицу для сетевого интерфейса overlay 10.10.10.1/24 и поместить 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

Таблица виртуальных таблиц маршрутизации отображается в шаблоне CPE и на устройстве:

- Для отображения таблицы виртуальных таблиц маршрутизации в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN → Шаблоны CPE**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **VRF**.

- Для отображения таблицы виртуальных таблиц маршрутизации на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **VRF**.

Информация о виртуальных таблицах маршрутизации отображается в следующих столбцах таблицы:

- **Имя** – имя виртуальной таблицы маршрутизации.
- **Таблица** – идентификатор виртуальной таблицы маршрутизации.
- **Интерфейсы** – сетевые интерфейсы, добавленные в виртуальную таблицу маршрутизации.

Создание виртуальной таблицы маршрутизации

Вы можете создать виртуальную таблицу маршрутизации в шаблоне CPE или на устройстве. Когда вы создаете виртуальную таблицу маршрутизации в шаблоне CPE, эта таблица автоматически создается на всех использующих шаблон устройствах.

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 и в отобразившейся области настройки выберите вкладку **VRF**.
   - Если вы хотите создать виртуальную таблицу маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **VRF**.

   Отобразится 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. В раскрывающемся списке **Интерфейсы** выберите ранее созданные сетевые интерфейсы, которые вы хотите добавить в таблицу маршрутизации. Вы не можете добавить один сетевой интерфейс в несколько виртуальных таблиц маршрутизации.

   Если вы добавляете 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.
6. Нажмите на кнопку **Создать**.

   Виртуальная таблица маршрутизации будет создана и отобразится в таблице.
7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

Изменение виртуальной таблицы маршрутизации

Вы можете изменить виртуальную таблицу маршрутизации в шаблоне CPE или на устройстве. Когда вы изменяете виртуальную таблицу маршрутизации в шаблоне CPE, эта таблица автоматически изменяется на всех использующих шаблон устройствах. Вы не можете изменить на устройстве CPE виртуальную таблицу маршрутизации, унаследованную из шаблона.

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 и в отобразившейся области настройки выберите вкладку **VRF**.

   - Если вы хотите изменить виртуальную таблицу маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **VRF**.

   Отобразится таблица виртуальных таблиц маршрутизации.

2. Нажмите на кнопку **Изменить** рядом с виртуальной таблицей маршрутизации, которую вы хотите изменить.

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. В раскрывающемся списке **Интерфейсы** выберите ранее созданные сетевые интерфейсы, которые вы хотите добавить в таблицу маршрутизации. Вы не можете добавить один сетевой интерфейс в несколько виртуальных таблиц маршрутизации.

   Если вы добавляете 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.

6. Нажмите на кнопку **Сохранить**.

   Виртуальная таблица маршрутизации будет изменена и обновится в таблице.

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

Удаление виртуальной таблицы маршрутизации

Вы можете удалить виртуальную таблицу маршрутизации в шаблоне CPE или на устройстве. Когда вы удаляете виртуальную таблицу маршрутизации в шаблоне CPE, эта таблица автоматически удаляется на всех использующих шаблон устройствах. Вы не можете удалить на устройстве CPE виртуальную таблицу маршрутизации, унаследованную из шаблона.

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 и в отобразившейся области настройки выберите вкладку **VRF**.

- Если вы хотите удалить виртуальную таблицу маршрутизации на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство и в отобразившейся области настройки выберите вкладку **VRF**.

Отобразится 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона CPE или устройства.

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.

Вам нужно указать основные параметры NetFlow в шаблоне NetFlow, после чего применить его к устройствам CPE при добавлении или ручной регистрации устройств, чтобы не настраивать каждое отдельное устройство. Если вы изменяете параметр в шаблоне NetFlow, этот параметр автоматически изменяется на всех использующих шаблон устройствах CPE. Если вы изменяете параметр NetFlow на устройстве CPE, этот параметр перестает зависеть от шаблона NetFlow. При изменении в шаблоне NetFlow такой параметр не изменяется 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 на сетевом интерфейсе при создании или изменении сетевого интерфейса.

Работа с шаблонами NetFlow

Для отображения таблицы шаблонов NetFlow вам нужно в меню перейти в раздел **SD-WAN → Шаблоны NetFlow**. Один из шаблонов является *шаблоном по умолчанию* – он предварительно выбран при добавлении и ручной регистрации устройства CPE. По умолчанию в портале администратора создан шаблон **Default NetFlow template**, на основании которого создаются все остальные шаблоны NetFlow. Тенантам нужно вручную создать и назначить шаблон NetFlow по умолчанию в портале самообслуживания.

Информация о шаблонах NetFlow отображается в следующих столбцах таблицы:

- **ID** – идентификатор шаблона NetFlow.

- **Имя** – имя шаблона NetFlow.

- **Использование** – используется ли шаблон 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 инструкции Работа с таблицами компонентов решения.

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.

Назначение шаблона NetFlow по умолчанию

Вы можете назначить шаблон NetFlow шаблоном по умолчанию, чтобы он был предварительно выбран при добавлении и ручной регистрации устройства CPE.

Чтобы назначить шаблон NetFlow по умолчанию:

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

   Отобразится таблица шаблонов NetFlow.

2. Нажмите на шаблон NetFlow, который вы хотите назначить шаблоном по умолчанию.

   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 **Назначить шаблоном по умолчанию**.

Шаблон NetFlow будет назначен шаблоном по умолчанию.

Экспорт шаблона NetFlow

Вы можете экспортировать шаблон NetFlow, чтобы затем импортировать его в другой шаблон.

Чтобы экспортировать 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.

Импорт шаблона NetFlow

Вы можете импортировать в шаблон NetFlow ранее экспортированный шаблон. Параметры шаблона NetFlow выстраиваются в соответствии с параметрами импортированного шаблона. При импорте можно выбрать параметры, которые вы хотите оставить без изменений.

Шаблон NetFlow, в который был импортирован другой шаблон, остается примененным к устройствам CPE, но параметры этих устройств 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, в который вы хотите импортировать другой шаблон.

   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 **Импортировать**.

4. В открывшемся окне снимите флажки рядом с параметрами шаблона NetFlow, которые вы хотите оставить без изменения после импорта.

5. В поле **Файл** укажите путь к архиву в формате TAR.GZ.

6. Нажмите на кнопку **Импортировать**.

Параметры шаблона NetFlow будут изменены в соответствии с параметрами импортируемого шаблона.

Клонирование шаблона NetFlow

Вы можете клонировать шаблон NetFlow, чтобы создать такой же шаблон 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**.

Копия шаблона NetFlow с новым именем будет создана и отобразится в таблице.

Просмотр использования шаблона NetFlow

Вы можете просмотреть, какие устройства CPE используют шаблон NetFlow. Если шаблон NetFlow используется хотя бы одним устройством CPE, этот шаблон невозможно удалить.

Чтобы просмотреть использование шаблона NetFlow:

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

   Отобразится таблица шаблонов NetFlow.

2. Нажмите на шаблон NetFlow, использование которого вы хотите просмотреть.

   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. Вам нужно просмотреть использование шаблона NetFlow и убедиться, что он не используется ни одним устройством CPE.

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. Когда вы настраиваете основные параметры NetFlow в шаблоне NetFlow, эти параметры автоматически распространяются на все использующие шаблон устройства CPE.

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.

   - Если вы хотите настроить основные параметры NetFlow на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **NetFlow** и установите флажок **Переопределить**.

   Отобразятся основные параметры NetFlow.

2. В раскрывающемся списке **NetFlow** выберите **Включено**. По умолчанию выбрано значение **Выключено**.

3. Укажите NetFlow-коллектор, выполнив следующие действия:

   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 несколько NetFlow-коллекторов и удалить коллектор, нажав рядом с ним на значок удаления ✕. Для одного устройства CPE можно указать не более четырех NetFlow-коллекторов.

4. В раскрывающемся списке **Версия экспорта** выберите версию протокола NetFlow:

   - **1**.
   - **5**.
   - **9** – значение по умолчанию.

5. В раскрывающемся списке **Уровень отслеживания** выберите, какую информацию о пакетах трафика устройство CPE должно отслеживать:

   - **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. Значение 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. По умолчанию указано значение `8192`.

   Чем выше введенное значение, тем выше нагрузка на процессор устройства CPE.

7. В поле **Частота выборки** введите, как часто устройство CPE должно отслеживать информацию о пакетах трафика. Например, если вы вводите `10`, устройство CPE отслеживает информацию о каждом десятом пакете трафика. Диапазон значений: от 1 до 8192. По умолчанию указано значение `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. По умолчанию указано значение `60`.

9. В поле **Лимит хопов** введите максимальное количество хопов до NetFlow-коллекторов. Диапазон значений: от 1 до 255. По умолчанию указано значение `64`.

10. Если вы хотите, чтобы устройство CPE отслеживало IPv6-трафик, в раскрывающемся списке **Отслеживать IPv6** выберите **Включено**. По умолчанию выбрано значение **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 на сетевом интерфейсе 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 → Устройства CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, шаблон NetFlow которого вы хотите изменить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В раскрывающемся списке **Шаблон NetFlow** выберите ранее 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 и статистику его работы, 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. Отчет с результатами работы утилиты отображается в веб-интерфейсе оркестратора.
- *Traceroute* – утилита для определения маршрута между устройством CPE и указанным IPv4-адресом. Отчет с результатами работы утилиты отображается в веб-интерфейсе оркестратора.
- *Tcpdump* – утилита для захвата трафика на устройстве CPE и записи этого трафика в файл отчета. При захвате с трафика снимается копия, и трафик продолжает передаваться до назначения. Файл с захваченным трафиком можно скачать и удалить.
- *Iperf* – утилита для диагностики производительности сети и записи результатов в файл отчета. Вы можете использовать устройство CPE как iperf-сервер или как iperf-клиента. Файл с результатами диагностики производительности сети можно скачать и удалить.
- *Sweep* – утилита для выполнения следующих действий на устройстве CPE:
  - очистка ARP-кеша;
  - перезапуск FRR-процесса (Free Range Routing);
  - очистка таблицы NAT-сессий.

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 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 должен автоматически выключиться.

Запрос диагностической информации

Чтобы запросить диагностическую информацию:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запросить диагностическую информацию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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**.

5. В раскрывающемся списке **Имя** выберите тип диагностической информации, которую вы хотите отобразить:

   - **disk usage** – информация об использовании диска устройства CPE. Значение по умолчанию.
   - **dump-flows** – информация об OpenFlow-потоках.
   - **dump-groups** – информация об OpenFlow-группах.
   - **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 intarfaces** – информация об интерфейсах SD-WAN.
- **modems** – информация модемах.
- **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 длинна: 64 символа. Если вы хотите, чтобы отобразились только строки без введенных слов, установите флажок **Выбрать несоответствующие строки**. По умолчанию флажок снят.

   b. В поле **Отображать N строк 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 файл с последними данными**.

   На ваше локальное устройство сохранится файл в формате TXT.

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 должен автоматически выключиться.

Чтобы включить интерактивный режим:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите включить интерактивный режим.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В верхней части области настройки нажмите на кнопку **Вкл. интеракт. режим**.

Интерактивный режим будет включен на устройстве CPE.

Запуск утилиты ping

Чтобы запустить утилиту ping:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту ping.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты**.

   По умолчанию будет выбрана вкладка **Ping**, на которой отображаются параметры утилиты ping.

4. В поле **IP-адрес назначения** введите IPv4-адрес, на который устройство CPE должно отправить ICMP-запросы.

5. Если вы хотите, чтобы устройство CPE отправило ICMP-запросы с указанного ранее созданного сетевого интерфейса, в раскрывающемся списке **Интерфейс источника** выберите сетевой интерфейс.

6. В поле **Количество** введите количество ICMP-запросов, которое устройство CPE должно отправить. Диапазон значений: от 1 до 1 000 000. По умолчанию указано значение `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. По умолчанию указано значение `2`.

8. В поле **Размер** введите размер ICMP-запроса в байтах. Диапазон значений: от 1 до 65 535. По умолчанию указано значение `56`

9. В поле **TTL** введите максимальное количество хопов для ICMP-запросов. Диапазон значений: от 1 до 255. По умолчанию указано значение `255`.

10. В поле **Интервал** введите интервал в секундах для отправки устройством CPE ICMP-запросов на указанный IPv4-адрес. Диапазон значений: от 1 до 300. По умолчанию указано значение `1`.

11. Нажмите на кнопку **Запустить**.

Утилита ping будет запущена на устройстве CPE, и отчет с результатами работы утилиты отобразится в нижней части области настройки.

Запуск утилиты traceroute

Чтобы запустить утилиту traceroute:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту traceroute.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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 должно отправить серию ICMP-запросов.

5. Если вы хотите, чтобы устройство CPE отправило серию ICMP-запросов с указанного ранее созданного сетевого интерфейса, в раскрывающемся списке **Интерфейс источника** выберите сетевой интерфейс.

6. Если вы хотите, чтобы при создании отчета с результатами работы утилиты 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. По умолчанию флажок снят.

7. В поле **Таймаут проб (сек.)** введите время в секундах, по прошествии которого устройство CPE должно получить серию ICMP-ответов, чтобы считать запрос успешным. Диапазон значений: от 1 до 30. По умолчанию указано значение `3`.

8. В поле **Макс. шагов** введите максимальное количество хопов для серии ICMP-запросов. Диапазон значений: от 1 до 60. По умолчанию указано значение `10`.

9. Нажмите на кнопку **Запустить**.

Утилита traceroute будет запущена на устройстве CPE, и отчет с результатами работы утилиты отобразится в нижней части области настройки.

Запуск утилиты tcpdump

Если вы уже запускали утилиту tcpdump, был сгенерирован файл отчета с захваченным трафиком. При повторном запуске утилиты файл отчета перезаписывается. Вы можете скачать предыдущий файл отчета, 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 → Устройства CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту tcpdump.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Tcpdump**.

   Отобразятся параметры утилиты tcpdump.

4. В раскрывающемся списке **Интерфейс для захвата** выберите ранее созданный сетевой интерфейс, на котором вы хотите захватывать трафик.

5. В раскрывающемся списке **Направление** выберите направление трафика, который вы хотите захватывать:

   - **вход** – захватывать входящий трафик.
   - **выход** – захватывать исходящий трафик.
   - **вход/выход** – захватывать входящий и исходящий трафик. Значение по умолчанию.

6. Если вы хотите, чтобы при создании файла 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 отображаются в файле отчета. По умолчанию флажок снят.

7. Если вы хотите использовать фильтр для захвата трафика, в поле **Выражение перехвата (в формате фильтра tcpdump)** введите синтаксис фильтра. Максимальная длина: 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 перехвата (сек.)** введите время в секундах, по прошествии которого захват трафика должен прекратиться. Диапазон значений: от 10 до 600. По умолчанию указано значение `30`.

9. В поле **Макс. Захваченных пакетов** введите количество пакетов трафика, при котором захват трафика должен прекратиться. Диапазон значений: от 1 до 10 000. По умолчанию указано значение `1000`.

Захват трафика прекращается по прошествии времени, указанного в поле **Максимальное время перехвата (сек.)**, или при захвате количества пакетов трафика, указанного в поле **Макс. Захваченных пакетов**.

10. Нажмите на кнопку **Запустить**.

Утилита tcpdump будет запущена на устройстве CPE, и будет сгенерирован файл отчета с захваченным трафиком.

Запуск утилиты iperf

Если вы уже запускали утилиту iperf, был сгенерирован файл отчета с результатами диагностики производительности сети. При повторном запуске утилиты файл отчета перезаписывается. Вы можете скачать предыдущий файл отчета, чтобы не потерять его.

Чтобы запустить утилиту iperf:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите запустить утилиту iperf.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке 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-клиента.

5. Если вы выбрали вариант **Сервер**, настройте iperf-сервер, выполнив следующие действия:

   a. В поле **Порт** введите номер порта TCP или UDP iperf-сервера. Диапазон значений: от 1001 до 65 535. По умолчанию указано значение `7777`.

   b. В поле **Интервал отчетов (сек.)** введите интервал в секундах для записи строчек в файл отчета. Диапазон значений: от 0 до 60. По умолчанию указано значение `3`.

   c. Если вы хотите не создавать файл отчета с результатами диагностики производительности сети, установите флажок **Не сообщать**. По умолчанию флажок снят.

   d. В блоке **Формат отчетов** выберите формат результатов диагностики производительности сети в файле отчета:

      - **Кбит/сек** – вариант 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. По умолчанию указано значение `300`.

6. Если вы выбрали вариант **Клиент**, настройте iperf-клиента, выполнив следующие действия:

a. В поле **IP сервера** введите IPv4-адрес iperf-сервера, к которому клиент должен подключиться.

b. В поле **Порт** введите номер порта TCP или UDP iperf-сервера, к которому клиент должен подключиться. Диапазон значений: от 1001 до 65 535. По умолчанию указано значение `7777`.

c. В поле **Интервал отчетов (сек.)** введите интервал в секундах для записи строчек в файл отчета с результатами диагностики производительности сети. Диапазон значений: от 0 до 60. По умолчанию указано значение `3`.

d. Если вы хотите не создавать файл отчета с результатами диагностики производительности сети, установите флажок **Не сообщать**. По умолчанию флажок снят.

e. В блоке **Формат отчетов** выберите формат результатов диагностики производительности сети в файле отчета:

- **Кбит/сек** – вариант 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. По умолчанию указано значение `60`.

g. Укажите тип порта iperf-сервера, выбрав один из следующих вариантов:

- **TCP** – вариант по умолчанию.
- **UDP**.

h. В поле **Битрейт клиента** введите скорость передачи данных iperf-клиентом в одном из следующих форматов:

- `<скорость в битах в секунду>`

  Например, если вы вводите `10000`, скорость передачи данных составляет 10 000 бит в секунду.

- `<скорость в килобитах в секунду>k`

  Например, если вы вводите `10k`, скорость передачи данных составляет 10 килобит в секунду.

- `<скорость в килобайтах в секунду>K`

  Например, если вы вводите `10K`, скорость передачи данных составляет 10 килобайт в секунду.

- `<скорость в мегабитах в секунду>m`

  Например, если вы вводите `10m`, скорость передачи данных составляет 10 мегабит в секунду.

- `<скорость в мегабайтах в секунду>M`

  Например, если вы вводите `10M`, скорость передачи данных составляет 10 мегабайт 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 серверу. Значение по умолчанию.
- **сервер-клиент** – использовать трафик, который iperf-сервер передает клиенту.
- **двунаправленный** – использовать трафик, который iperf-клиент передает серверу и iperf-сервер передает клиенту.

j. При необходимости в поле **Размер окна TCP, байт** введите размер TCP-окна в байтах. Если вы не указываете значение для этого параметра, 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 файл отчета с результатами диагностики производительности сети.

Вы можете перейти к работе с файлом отчета, нажав на кнопку **Скачать файл**.

Запуск утилиты sweep

Вы можете очистить ARP-кеш, перезапустить FRR-процесс (Free Range Routing) и очистить таблицу NAT-сессий на устройстве CPE с помощью утилиты sweep.

Перезапуск FRR-процесса 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 → Устройства CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, котором вы хотите запустить утилиту sweep.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Очистка**.

   Отобразятся параметры утилиты sweep.

4. Если вы хотите очистить ARP-кеш, выполните следующие действия:

   a. В блоке **Очистить кеш ARP на интерфейсе** выберите ранее 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 FRR-процесс, в блоке **Перезапустить процесс FRR (маршрутизация)** нажмите на кнопку **Запустить**.

   FRR-процесс будет перезапущен на устройстве CPE.

6. Если вы хотите очистить таблицу NAT-сессий, в блоке **Очистить таблицу сессий NAT** нажмите на кнопку **Запустить**. Вы можете настроить NAT на устройстве CPE с помощью межсетевого экрана.

   Таблица NAT-сессий будет очищена на устройстве CPE.

Работа с файлами отчета

Файлы отчета генерируются в результате работы утилит tcpdump и iperf. Для отображения таблицы файлов отчета на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Утилиты → Файлы**. Информация о файлах отчета отображается в следующих столбцах таблицы:

- **Тип** – тип файла отчета.
- **Создан** – дата и время создания файла отчета.

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

Скачивание файла отчета

Чтобы скачать файл отчета:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, с которого вы хотите скачать файл отчета.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты → Файлы**.

   Отобразится таблица файлов отчета.

4. Нажмите на кнопку **Загрузить файл** рядом с файлом отчета, который вы хотите скачать.

На ваше локальное устройство сохранится файл в формате TXT.

Удаление файла отчета

Удаленные файлы отчета невозможно восстановить.

Чтобы удалить файл отчета:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, на котором вы хотите удалить файл отчета.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Утилиты** → **Файлы**.

   Отобразится таблица файлов отчета.

4. Нажмите на кнопку **Удалить** рядом с файлом отчета, который вы хотите удалить.

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

Файл отчета будет удален и перестанет отображаться в таблице.

Диапазоны IP-адресов и подсетей для устройств CPE

Вы можете создать диапазоны IP-адресов и подсетей для централизованного назначения IPv4-адресов сетевым интерфейсам при создании или изменении этих интерфейсов. 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 отображения таблицы диапазонов IP-адресов вам нужно в меню перейти в раздел **SD-WAN → IPAM**. По умолчанию будет выбрана вкладка **Пул 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 значение 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 инструкции 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 будет выбрана вкладка **Пул IP**, на которой отображается таблица диапазонов IP-адресов.

2. В верхней части страницы нажмите на кнопку **+ Пул IP**.
3. В открывшемся окне в поле **Имя** введите имя диапазона IP-адресов. Максимальная длина: 32 символа.
4. В поле **CIDR** введите IPv4-префикс подсети, в которой находится диапазон IP-адресов.
5. Укажите диапазон IP-адресов, выполнив следующие действия:

   a. В блоке **Диапазон IP** нажмите на кнопку **+ Добавить**.

   b. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

   Диапазон IP-адресов будет указан и отобразится в блоке **Диапазон IP**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав 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 будет выбрана вкладка **Пул IP**, на которой отображается таблица диапазонов IP-адресов.

2. Нажмите на диапазон IP-адресов, 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 будет выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона IP-адресов.

3. В открывшемся окне в поле **Имя** введите имя диапазона IP-адресов. Максимальная длина: 32 символа.

4. В поле **CIDR** введите IPv4-префикс подсети, в которой находится диапазон IP-адресов.

5. Укажите диапазон IP-адресов, выполнив следующие действия:

   a. В блоке **Диапазон IP** нажмите на кнопку **+ Добавить**.

   b. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

   Диапазон IP-адресов будет указан и отобразится в блоке **Диапазон IP**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав рядом с ним на значок удаления .

6. В верхней части области настройки нажмите на кнопку **Сохранить**.

Диапазон IP-адресов будет изменен и обновится в таблице.

Просмотр использования диапазона IP-адресов

Вы можете просмотреть, какие шаблоны CPE и устройства используют диапазон IP-адресов. Если диапазон IP-адресов используется хотя бы одним шаблоном CPE или устройством, этот диапазон невозможно удалить. Вы также можете просмотреть информацию об IP-адресах, которые были назначены из диапазона.

Чтобы просмотреть использование диапазона IP-адресов:

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

   По умолчанию будет выбрана вкладка **Пул IP**, на которой отображается таблица диапазонов IP-адресов.

2. Нажмите на диапазон IP-адресов, использование которого вы хотите просмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона IP-адресов.

3. При необходимости выполните одно из следующих действий:

   - Если вы хотите просмотреть, какие устройства CPE используют диапазон IP-адресов, выберите вкладку **Использование → CPE**.

     Отобразится список устройств CPE, использующих диапазон IP-адресов.

- Если вы хотите просмотреть, какие шаблоны CPE используют диапазон IP-адресов, выберите вкладку **Использование** → **Шаблон**.

  Отобразится список шаблонов CPE, использующих диапазон IP-адресов.

4. Если вы хотите просмотреть информацию об IP-адресах, которые были назначены из диапазона, выберите вкладку **Аренда**.

   Отобразится таблица IP-адресов, назначенных из диапазона. Информация об IP-адресах отображается в следующих столбцах таблицы:

   - **IP** – IP-адрес, который был назначен из диапазона.
   - **CPE** – устройство CPE, которому был назначен IP-адрес.
   - **Тип** – 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 назначено устройство CPE.

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

Удаление диапазонов IP-адресов

Вы не можете удалить диапазон IP-адресов, если он используется хотя бы одним шаблоном CPE или устройством. Вам нужно просмотреть использование диапазона IP-адресов и убедиться, что он не используется ни одним компонентом.

Удаленные диапазоны IP-адресов невозможно восстановить.

Чтобы удалить диапазоны IP-адресов:

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

   По умолчанию будет выбрана вкладка **Пул 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 будет 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 отображения таблицы диапазонов подсетей вам нужно в меню перейти в раздел **SD-WAN → IPAM** и выбрать вкладку **Пул 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 инструкции Работа с таблицами компонентов решения.

Создание диапазона подсетей

Чтобы создать диапазон подсетей:

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

   По умолчанию будет выбрана вкладка **Пул IP**, на которой отображается таблица диапазонов IP-адресов.

2. Выберите вкладку **Пул подсетей**.

   Отобразится таблица диапазонов подсетей.

3. В верхней части страницы нажмите на кнопку **+ Пул подсетей**.
4. В открывшемся окне в поле **Имя** введите имя диапазона подсетей. Максимальная длина: 32 символа.
5. В поле **Базовый CIDR** введите IPv4-префикс диапазона подсетей.
6. В поле **Суб-префикс** введите длину IPv4-префикса подсетей в диапазоне. 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 будет выбрана вкладка **Пул IP**, на которой отображается таблица диапазонов IP-адресов.

2. Выберите вкладку **Пул 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 будет выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона подсетей.

4. В открывшемся окне в поле **Имя** введите имя диапазона подсетей. Максимальная длина: 32 символа.

5. В поле **Базовый CIDR** введите IPv4-префикс диапазона подсетей.

6. В поле **Суб-префикс** введите длину IPv4-префикса подсетей в диапазоне. Диапазон значений: от 0 до 32.

7. В верхней части области настройки нажмите на кнопку **Сохранить**.

Диапазон подсетей будет изменен и обновится в таблице.

Просмотр использования диапазона подсетей

Вы можете просмотреть, какие шаблоны CPE и устройства используют диапазон подсетей. Если диапазон подсетей используется хотя бы одним шаблоном CPE или устройством, этот диапазон невозможно удалить. Вы также можете просмотреть информацию о подсетях, которые были назначены из диапазона.

Чтобы просмотреть использование диапазона подсетей:

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

   По умолчанию будет выбрана вкладка **Пул IP**, на которой отображается таблица диапазонов IP-адресов.

2. Выберите вкладку **Пул подсетей**.

   Отобразится таблица диапазонов подсетей.

3. Нажмите на диапазон подсетей, использование которого вы хотите просмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображаются параметры диапазона подсетей.

4. При необходимости выполните одно из следующих действий:

   - Если вы хотите просмотреть, какие устройства CPE используют диапазон подсетей, выберите вкладку **Использование → CPE**.

     Отобразится список устройств CPE, использующих диапазон подсетей.

   - Если вы хотите просмотреть, какие шаблоны CPE используют диапазон подсетей, выберите вкладку **Использование → Шаблон**.

     Отобразится список шаблонов CPE, использующих диапазон подсетей.

5. Если вы хотите просмотреть информацию о подсетях, которые были назначены из диапазона, выберите вкладку **Аренда**.

   Отобразится таблица подсетей, назначенных из диапазона. Информация о подсетях отображается в следующих столбцах таблицы:

   - **CIDR** – IPv4-префикс подсети, которая была назначена из диапазона.

- **CPE** – устройство CPE, которому был назначен IPv4-адрес из подсети.
- **Имя** – имя сетевого интерфейса, которому был назначен IPv4-адрес из подсети.
- **Тенант** – тенант, которому назначено устройство CPE.

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

Удаление диапазонов подсетей

Вы не можете удалить диапазон подсетей, если он используется хотя бы одним шаблоном CPE или устройством. Вам нужно просмотреть использование диапазона подсетей и убедиться, что он не используется ни одним компонентом.

Удаленные диапазоны подсетей невозможно восстановить.

Чтобы удалить диапазоны подсетей:

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

   По умолчанию будет выбрана вкладка **Пул IP**, на которой отображается таблица диапазонов IP-адресов.

2. Выберите вкладку **Пул 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 будет 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

Kaspersky SD-WAN поддерживает межсетевой экран (англ. firewall) для фильтрации пакетов трафика на устройстве CPE. Межсетевой экран может принимать (англ. accept), отбрасывать (англ. drop) и отклонять (англ. reject) пакеты трафика. При отклонении пакета трафика отправитель получает сообщение `icmp-reject`. Каждое из действий межсетевой экран может применять ко входящим и исходящим пакетам трафика, а также к пакетам трафика, перенаправляемым между сетевыми интерфейсами и подсетями.

Вам нужно указать параметры межсетевого экрана в шаблоне межсетевого экрана, после чего применить его к устройствам CPE при добавлении или ручной регистрации устройств, чтобы не настраивать каждое отдельное устройство. Если вы изменяете параметр межсетевого экрана в шаблоне, этот параметр автоматически изменяется на всех использующих шаблон устройствах CPE. Если вы изменяете параметр межсетевого экрана на устройстве CPE, этот параметр перестает зависеть от шаблона межсетевого экрана. При изменении в шаблоне межсетевого экрана такой параметр не изменяется на устройстве CPE.

Для выполнения действий с пакетами трафика, передающимися через сетевые интерфейсы и подсети, вам нужно поместить эти сетевые интерфейсы и подсети в *зону межсетевого экрана* (англ. firewall zone, далее также зона). Вы можете создать общие зоны, которые могут использовать несколько устройств CPE, и зоны на отдельном устройстве. При создании зоны вы указываете, какие действия должны выполняться с пакетами трафика и добавляете в нее подсети. Сетевые интерфейсы можно добавить в зону при создании или изменении этих интерфейсов. Для разрешения или запрета передачи трафика между двумя зонами можно создать *передачу* (англ. forwarding).

Вы не можете изменить общую зону, так как она может использоваться большим количеством шаблонов CPE и устройств, и изменение такой зоны привело бы к массовому обновлению всех использующих ее компонентов и перегрузке оркестратора. Если вы хотите изменить общую зону, вам нужно создать новую общую зону. В созданную общую зону необходимо добавить сетевые интерфейсы и подсети, которые были добавлены в предыдущую общую зону.

Для выполнения действий с пакетами трафика на основании указанных критериев вам нужно создать *правила межсетевого экрана*. Например, вы можете создать правило межсетевого экрана, которое отклоняет пакеты трафика с указанной вами зоной источника. При необходимости указать в нескольких правилах межсетевого экрана одинаковые IP-адреса или подсети можно создать *набор IP* (англ. IP set).

Когда пакет трафика передается на устройство CPE, к этому пакету трафика применяется одно из правил межсетевого экрана. Если ни одно из правил межсетевого экрана не может быть применено, с пакетом трафика выполняется действие, указанное в параметрах зоны, в которую был передан этот пакет. Если пакет трафика не был передан ни в одну из зон, с ним выполняется действие по умолчанию, которое вы указываете при настройке основных параметров межсетевого экрана.

Межсетевой экран поддерживает следующие механизмы трансляции сетевых адресов (англ. network address translation, NAT):

- *DNAT-правила* – могут заменять следующие элементы пакетов трафика указанными вами значениями:
  - IP-адреса или префиксы назначения;
  - зоны назначения;
  - порты назначения (Port Address Translation, PAT).
- *SNAT-правила* – могут заменять IP-адреса или префиксы источника пакетов трафика указанными вами 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.

Работа с зонами межсетевого экрана

Работа с общими зонами межсетевого экрана

Для отображения таблицы общих зон межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN** → **Зоны межсетевого экрана**. Информация о зонах межсетевого экрана отображается в следующих столбцах таблицы:

- **Имя** – имя зоны межсетевого экрана.
- **Использование** – используется ли зона шаблонами межсетевого экрана, шаблонами CPE и устройствами:
  - **Да**.
  - **Нет**.
- **Author** – имя пользователя, создавшего зону межсетевого экрана.
- **Создан** – дата и время создания зоны межсетевого экрана.

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

Работа с зонами межсетевого экрана на устройстве CPE

Для отображения таблицы зон межсетевого экрана на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Параметры межсетевого экрана** → **Зоны**. Информация о зонах межсетевого экрана отображается в следующих столбцах таблицы:

- **Имя** – имя зоны межсетевого экрана.
- **Параметры** – действия, которые межсетевой экран должен выполнять с пакетами трафика.
- **Интерфейсы/Сети** – сетевые интерфейсы и подсети, добавленные в зону межсетевого экрана.

Создание зоны межсетевого экрана

Вы можете создать общую зону межсетевого экрана или зону 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 → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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: 255 символов.

3. В раскрывающемся списке **Вход** выберите действие, которое межсетевой экран должен выполнять со входящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Значение по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

4. В раскрывающемся списке **Выход** выберите действие, которое межсетевой экран должен выполнять с исходящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Значение по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

5. В раскрывающемся списке **Передача** выберите действие, которое межсетевой экран должен выполнять с пакетами трафика, перенаправляемым между сетевыми интерфейсами и подсетями:

   - **ACCEPT** – принимать пакеты трафика. Значение по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

6. Если вы хотите заменять IP-адрес источника исходящих из зоны пакетов трафика на IP-адрес, назначенный исходящему (англ. egress) сетевому интерфейсу, выполните следующие действия:

   a. Установите флажок **Маскарадинг**. По умолчанию флажок снят.

   b. Если вы хотите заменять IP-адрес источника только пакетов трафика с указанной подсетью источника, выполните следующие действия:

      1. В блоке **Маскарадинг подсетей источника** нажмите на кнопку **+ Добавить**.
      2. В отобразившемся поле введите IPv4-префикс.

      Подсеть будет указана и отобразится в блоке **Маскарадинг подсетей источника**. Вы можете указать несколько подсетей и удалить подсеть, нажав рядом с ней на значок удаления ✕.

   c. Если вы хотите заменять IP-адрес источника только пакетов трафика с указанной подсетью назначения, выполните следующие действия:

      1. В блоке **Маскарадинг подсетей назначения** нажмите на кнопку **+ Добавить**.

2. В отобразившемся поле введите IPv4-префикс.

Подсеть будет указана и отобразится в блоке **Маскарадинг подсетей назначения**. Вы можете указать несколько подсетей и удалить подсеть, нажав рядом с ней на значок удаления ✕.

7. Если вы не хотите, чтобы межсетевой экран ограничивал значение MSS (Maximum Segment Size) передающихся через зону 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. По умолчанию флажок установлен.

8. Если вы хотите, чтобы межсетевой экран вел журнал отброшенных в зоне пакетов трафика, установите флажок **Журналировать drop-ы**. Если созданные на устройстве CPE журналы отправляются на Syslog-сервер, вы можете просмотреть журналы на этом сервере. Если созданные на устройстве CPE журналы хранятся локально, вы можете просмотреть журналы, запросив диагностическую информацию. По умолчанию флажок снят.

9. Если сетевые интерфейсы устройств CPE подключены к коммутаторам или маршрутизаторам L3, и вы хотите передавать через зону межсетевого экрана пакеты трафика из подсетей этих коммутаторов или маршрутизаторов, добавьте в зону подсеть, выполнив следующие действия:

   a. В блоке **Сети** нажмите на кнопку **+ Добавить**.

   b. В отобразившемся поле введите IPv4-префикс подсети.

   Подсеть будет добавлена и отобразится в блоке **Сети**. Вы можете добавить несколько подсетей и удалить подсеть, нажав 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.

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 только созданные на этом устройстве сетевые интерфейсы.

Изменение имени общей зоны межсетевого экрана

Вы можете изменить имя ранее созданной общей зоны межсетевого экрана. Изменение имени зоны межсетевого экрана на устройстве CPE, описано в инструкции по изменению зоны межсетевого экрана на устройстве CPE.

Чтобы изменить имя общей зоны межсетевого экрана:

1. В меню перейдите в раздел **SD-WAN → Зоны межсетевого экрана**.

   Отобразится таблица зон межсетевого экрана.

2. Нажмите на общую зону межсетевого экрана, имя которой вы хотите изменить.

   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 **Переименовать зону**.

4. В открывшемся окне введите новое имя общей зоны межсетевого экрана.

5. Нажмите на кнопку **Переименовать**.

Имя общей зоны межсетевого экрана будет изменено и обновится в таблице.

Клонирование общей зоны межсетевого экрана

Вы можете клонировать ранее 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 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**.

Копия общей зоны межсетевого экрана с новым именем будет создана и отобразится в таблице.

Просмотр использования общей зоны межсетевого экрана

Вы можете просмотреть, какие шаблоны межсетевого экрана, а также шаблоны CPE и устройства используют ранее созданную общую зону. Если общая зона межсетевого экрана используется хотя бы одним компонентом, эту зону невозможно удалить.

Чтобы просмотреть использование общей зоны межсетевого экрана:

1. В меню перейдите в раздел **SD-WAN → Зоны межсетевого экрана**.

   Отобразится таблица зон межсетевого экрана.

2. Нажмите на общую зону межсетевого экрана, использование которой вы хотите просмотреть.

   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, использующих общую зону.

Изменение зоны межсетевого экрана на устройстве CPE

Вы можете изменить ранее созданную на устройстве CPE зону межсетевого экрана.

Вы не можете изменить общую зону, так как она может использоваться большим количеством шаблонов CPE и устройств, и изменение такой зоны привело бы к массовому обновлению всех использующих ее компонентов и перегрузке оркестратора. Если вы хотите изменить общую зону, вам нужно создать новую общую зону. В созданную общую зону необходимо добавить сетевые интерфейсы и подсети, которые были добавлены в предыдущую общую зону.

Чтобы изменить зону межсетевого экрана на устройстве CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Параметры межсетевого экрана → Зоны**.

   Отобразится таблица зон межсетевого экрана.

4. Установите флажок **Переопределить**.

5. Нажмите на кнопку **Изменить** рядом с зоной, которую вы хотите изменить.

6. В открывшемся окне в поле **Имя** введите имя зоны межсетевого экрана. Максимальная длина: 255 символов.

7. В раскрывающемся списке **Вход** выберите действие, которое межсетевой экран должен выполнять со входящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Значение по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

8. В раскрывающемся списке **Выход** выберите действие, которое межсетевой экран должен выполнять с исходящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Значение по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

9. В раскрывающемся списке **Передача** выберите действие, которое межсетевой экран должен выполнять с пакетами трафика, перенаправляемым между сетевыми интерфейсами и подсетями:

   - **ACCEPT** – принимать пакеты трафика. Значение по умолчанию.
   - **DROP** – отбрасывать пакеты трафика.
   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

10. Если вы хотите заменять IP-адрес источника исходящих из зоны пакетов трафика на IP-адрес, назначенный исходящему (англ. egress) сетевому интерфейсу, выполните следующие действия:

    a. Установите флажок **Маскарадинг**. По умолчанию флажок снят.

    b. Если вы хотите заменять IP-адрес источника только пакетов трафика с указанной подсетью источника, выполните следующие действия:

        1. В блоке **Маскарадинг подсетей источника** нажмите на кнопку **+ Добавить**.

        2. В отобразившемся поле введите IPv4-префикс.

        Подсеть будет указана и отобразится в блоке **Маскарадинг подсетей источника**. Вы можете указать несколько подсетей и удалить подсеть, нажав рядом с ней на значок удаления ✕.

    c. Если вы хотите заменять IP-адрес источника только пакетов трафика с указанной подсетью назначения, выполните следующие действия:

        1. В блоке **Маскарадинг подсетей назначения** нажмите на кнопку **+ Добавить**.

        2. В отобразившемся поле введите IPv4-префикс.

        Подсеть будет указана и отобразится в блоке **Маскарадинг подсетей назначения**. Вы можете указать несколько подсетей и удалить подсеть, нажав рядом с ней на значок удаления ✕.

11. Если вы не хотите, чтобы межсетевой экран ограничивал значение MSS (Maximum Segment Size) передающихся через зону 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. По умолчанию флажок установлен.

12. Если вы хотите, чтобы межсетевой экран вел журнал отброшенных в зоне пакетов трафика, установите флажок **Журналировать drop-ы**. Если созданные на устройстве CPE журналы отправляются на Syslog-сервер, вы можете просмотреть журналы на этом сервере. Если созданные на устройстве CPE журналы хранятся локально, вы можете просмотреть журналы, запросив диагностическую информацию. По умолчанию флажок снят.

13. Если сетевые интерфейсы устройств CPE подключены к коммутаторам или маршрутизаторам L3, и вы хотите передавать через зону межсетевого экрана пакеты трафика из подсетей этих коммутаторов или маршрутизаторов, добавьте в зону подсеть, выполнив следующие действия:

    a. В блоке **Сети** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите IPv4-префикс подсети.

    Подсеть будет добавлена и отобразится в блоке **Сети**. Вы можете добавить несколько подсетей и удалить подсеть, нажав рядом с ней на значок удаления ✕.

14. Нажмите на кнопку **Сохранить**.

    Зона межсетевого экрана будет изменена и обновится в таблице.

15. 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 на устройстве CPE.

Удаленные зоны межсетевого экрана невозможно восстановить.

Удаление общей зоны межсетевого экрана

Вы не можете удалить общую зону, если она используется хотя бы одним шаблоном межсетевого экрана, шаблоном CPE или устройством. Вам нужно просмотреть использование общей зоны межсетевого экрана и убедиться, что она не используется ни одним компонентом.

Чтобы удалить общую зону межсетевого экрана:

1. В меню перейдите в раздел **SD-WAN → Зоны межсетевого экрана**.

   Отобразится таблица 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 → Устройства CPE**.

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. Выберите вкладку **Параметры межсетевого экрана → 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

Таблица шаблонов межсетевого экрана отображается в разделе **SD-WAN → Шаблоны межсетевого экрана**. Один из шаблонов является *шаблоном по умолчанию* – он предварительно выбран при добавлении и ручной регистрации устройства CPE. По умолчанию создан шаблон **Default firewall template**, на основании которого создаются все остальные шаблоны межсетевого экрана. Информация о шаблонах межсетевого экрана отображается в следующих столбцах таблицы:

- **Имя** – имя шаблона межсетевого экрана.
- **Использование** – используется ли шаблон межсетевого экрана устройствами CPE:
  - **Да**.
  - **Нет**.
- **Владелец** – имя пользователя, создавшего шаблон межсетевого экрана.
- **Последнее обновление** – дата и время последнего изменения параметров шаблона межсетевого экрана.

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

Параметры шаблона межсетевого экрана отображаются на следующих вкладках:

- **Глобальные настройки** – основные параметры межсетевого экрана.
- **Правила** – правила межсетевого экрана.
- **NAT** – параметры NAT. На этой вкладке отображаются следующие вкладки:
  - **DNAT** – DNAT-правила.
  - **SNAT** – SNAT-правила.
- **Передачи между зонами** – передачи между зонами.
- **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.

Назначение шаблона межсетевого экрана по умолчанию

Вы можете назначить шаблон межсетевого экрана шаблоном по умолчанию, чтобы он был предварительно выбран при добавлении и ручной регистрации устройства CPE.

Чтобы назначить шаблон межсетевого экрана по умолчанию:

1. Перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**.

   Отобразится таблица шаблонов межсетевого экрана.

2. Нажмите на шаблон межсетевого экрана, который вы хотите назначить шаблоном по умолчанию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Глобальные настройки**, на которой отображаются основные параметры шаблона межсетевого экрана.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Назначить шаблоном по умолчанию**.

Шаблон межсетевого экрана будет назначен шаблоном по умолчанию.

Экспорт шаблона межсетевого экрана

Вы можете экспортировать шаблон межсетевого экрана, чтобы затем импортировать его в другой шаблон.

Чтобы экспортировать 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 будет выбрана вкладка **Глобальные настройки**, 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.

Импорт шаблона межсетевого экрана

Вы можете импортировать в шаблон межсетевого экрана ранее экспортированный шаблон. Параметры шаблона межсетевого экрана выстраиваются в соответствии с параметрами импортированного шаблона. При импорте можно выбрать вкладки, которые вы хотите оставить без изменений.

Шаблон межсетевого экрана, в который был импортирован другой шаблон, остается примененным к устройствам CPE, но параметры этих устройств 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, в который вы хотите импортировать другой шаблон.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Глобальные настройки**, на которой отображаются основные параметры шаблона межсетевого экрана.

3. В верхней части области настройки в блоке **Действия** нажмите на кнопку **Импортировать**.

4. В открывшемся окне снимите флажки рядом с вкладками шаблона межсетевого экрана, которые вы хотите оставить без изменения после импорта.

5. В поле **Файл** укажите путь к архиву в формате TAR.GZ.

6. Нажмите на кнопку **Импортировать**.

   Параметры шаблона межсетевого экрана будут изменены в соответствии с параметрами импортируемого шаблона.

Клонирование шаблона межсетевого экрана

Вы можете клонировать шаблон межсетевого экрана, чтобы создать такой же шаблон 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 будет выбрана вкладка **Глобальные настройки**, 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**.

   Копия шаблона межсетевого экрана с новым именем будет создана и отобразится в таблице.

Просмотр использования шаблона межсетевого экрана

Вы можете просмотреть, какие устройства CPE используют шаблон межсетевого экрана. Если шаблон межсетевого экрана используется хотя бы одним устройством CPE, этот шаблон невозможно удалить.

Чтобы просмотреть использование шаблона 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 просмотреть.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Глобальные настройки**, 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. Вам нужно просмотреть использование шаблона межсетевого экрана и убедиться, что он не используется ни одним устройством CPE.

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 будет выбрана вкладка **Глобальные настройки**, 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. Когда вы настраиваете основные параметры межсетевого экрана в шаблоне, эти параметры автоматически распространяются на все использующие шаблон устройства CPE.

Межсетевой экран применяет к пакетам трафика действия, указанные в основных параметрах. 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 экрана в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN** → **Шаблоны межсетевого экрана** и нажмите на шаблон.

   - Если вы хотите настроить основные параметры межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана** → **Глобальные настройки** и установите флажок **Переопределить**.

   Отобразятся основные параметры межсетевого экрана.

2. Если вы хотите выключить защиту от SYN-флуда, снимите флажок **Защита от Syn-flood**. По умолчанию флажок установлен. 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**. По умолчанию флажок снят.

4. Если вы хотите выключить использование технологии DPI (Deep Packet Inspection), снимите флажок **Включить DPI**. По умолчанию флажок установлен. С помощью технологии DPI вы можете создавать правила межсетевого экрана, которые применяются только к пакетам трафика указанного вами приложения.

   Когда использование технологии DPI выключено, вы не можете настроить маркировку DPI, и правила межсетевого экрана, которые используют эту технологию, автоматически выключаются.

5. В раскрывающемся списке **INPUT-действие по умолчанию** выберите действие, которое межсетевой экран должен выполнять со входящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Значение 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 должен выполнять с исходящими пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Значение 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 должен выполнять с пакетами трафика, перенаправленными между сетевыми интерфейсами и подсетями:

   - **ACCEPT** – принимать пакеты трафика. Значение по умолчанию.

   - **DROP** – отбрасывать пакеты трафика.

   - **REJECT** – отклонять пакеты трафика с сообщением `icmp-reject`.

8. В верхней 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 вами приложения. Вы можете указать марки DPI, на основании которых такие правила должны применяться к пакетам трафика.

Маркировку DPI можно настроить в шаблоне межсетевого экрана или на устройстве CPE. Когда вы настраиваете маркировку DPI в шаблоне межсетевого экрана, эти параметры автоматически распространяются на все использующие шаблон устройства CPE.

Вы не можете настроить маркировку DPI, если вы выключили использование технологии DPI при настройке основных параметров межсетевого экрана.

Чтобы настроить маркировку DPI для межсетевого экрана:

1. Перейдите к настройке маркировки DPI для межсетевого экрана одним из следующих способов:

   - Если вы хотите настроить маркировку DPI для межсетевого экрана в шаблоне межсетевого экрана, в меню перейдите в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажмите на шаблон и в отобразившейся области настройки выберите вкладку **Маркировка DPI**.

   - Если вы хотите настроить маркировку DPI для межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → Маркировка DPI** и установите флажок **Переопределить**.

   Отобразятся параметры маркировки DPI.

2. Установите флажки рядом с марками DPI, на основании которых правила межсетевого экрана должны применяться к пакетам трафика.

3. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с правилами межсетевого экрана

Таблица правил межсетевого экрана отображается в шаблоне межсетевого экрана и на устройстве CPE:

- Для отображения таблицы правил межсетевого экрана в шаблоне межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Правила**.

- Для отображения таблицы правил межсетевого экрана на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Параметры межсетевого экрана → Правила**.

Информация о правилах межсетевого экрана отображается в следующих столбцах таблицы:

- **Имя** – имя правила межсетевого экрана.

- **Детали** – критерии, согласно которым межсетевой экран должен применять правило к пакетам трафика.
- **Действие** – действие, которое правило межсетевого экрана должно выполнять с пакетами трафика.

Создание правила межсетевого экрана

Вы можете создать правило межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Когда вы создаете правило межсетевого экрана в шаблоне, это правило автоматически создается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Правила**.
   - Если вы хотите создать правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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: 255 символов.
4. В раскрывающемся списке **Действие** выберите действие, которое правило межсетевого экрана должно выполнять с пакетами трафика:
   - **ACCEPT** – принимать пакеты трафика. Значение 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. 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 должен применять правило 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 ранее 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 указанной версией IP-адресов или подсетей источника или назначения, в раскрывающемся списке **Версия IP** выберите одно из следующих значений:
      - **IPv4**.

- **IPv6**.

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 источника, в раскрывающемся списке **Зона источника** выберите ранее созданную зону.

d. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанной зоной назначения, в раскрывающемся списке **Зона назначения** выберите ранее созданную зону.

e. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанным IPv4-адресом или префиксом источника, выполните следующие действия:

1. В блоке **IP источника** нажмите на кнопку **+ Добавить**.
2. В отобразившемся поле введите IPv4-адрес или префикс.

IPv4-адрес или префикс источника будет указан и отобразится в блоке **IP источника**. Вы можете указать несколько IPv4-адресов или префиксов и удалить IPv4-адрес или префикс, нажав 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, выполните следующие действия:

1. В блоке **IP назначения** нажмите на кнопку **+ Добавить**.
2. В отобразившемся поле введите IPv4-адрес или префикс.

IPv4-адрес или префикс назначения будет указан и отобразится в блоке **IP назначения**. Вы можете указать несколько IPv4-адресов или префиксов и удалить IPv4-адрес или префикс, нажав 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 вы 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 должно применяться к пакетам трафика. Если вы выключили использование технологии DPI при настройке основных параметров межсетевого экрана, правило автоматически выключается.

6. Нажмите на кнопку **Создать**.

   Правило межсетевого экрана будет создано и отобразится в таблице.

7. В верхней 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 в верхней части таблицы. По умолчанию правила межсетевого экрана отображаются в таблице в порядке создания. Чем раньше правило было создано, тем выше оно отображается в таблице.

Вы можете настроить порядок применения правил межсетевого экрана в шаблоне межсетевого экрана или на устройстве CPE. Когда вы настраиваете порядок применения правил межсетевого трафика в шаблоне, этот порядок автоматически распространяется на все использующие шаблон устройства CPE.

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 и в отобразившейся области настройки выберите вкладку **Правила**.

   - Если вы хотите настроить порядок применения правил межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана** → **Правила** и установите флажок **Переопределить**.

   Отобразится таблица правил межсетевого экрана.

2. Настройте порядок применения правил межсетевого экрана, нажимая рядом с ними на кнопки **UP** и **DOWN**.

3. В верхней 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. Когда вы изменяете правило межсетевого экрана в шаблоне, это правило автоматически изменяется на всех использующих шаблон устройствах CPE.

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 и в

отобразившейся области настройки выберите вкладку **Правила**.

- Если вы хотите изменить правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 в поле **Имя** введите имя правила межсетевого экрана. Максимальная длина: 255 символов.

4. В раскрывающемся списке **Действие** выберите действие, которое правило межсетевого экрана должно выполнять с пакетами трафика:

   - **ACCEPT** – принимать пакеты трафика. Значение 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. 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 должен применять правило 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 ранее 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 указанной версией IP-адресов или подсетей источника или назначения, в раскрывающемся списке **Версия IP** выберите одно из следующих значений:

      - **IPv4**.
      - **IPv6**.

      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 источника, в раскрывающемся списке **Зона источника** выберите ранее созданную зону.

   d. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанной зоной назначения, в раскрывающемся списке **Зона назначения** выберите ранее созданную зону.

   e. Если вы хотите применять правило межсетевого экрана только к пакетам трафика с указанным IPv4-адресом или префиксом источника, выполните следующие действия:

      1. В блоке **IP источника** нажмите на кнопку **+ Добавить**.
      2. В отобразившемся поле введите IPv4-адрес или префикс.

IPv4-адрес или префикс источника будет указан и отобразится в блоке **IP источника**. Вы можете указать несколько IPv4-адресов или префиксов и удалить IPv4-адрес или префикс, нажав 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, выполните следующие действия:

1. В блоке **IP назначения** нажмите на кнопку **+ Добавить**.
2. В отобразившемся поле введите IPv4-адрес или префикс.

IPv4-адрес или префикс назначения будет указан и отобразится в блоке **IP назначения**. Вы можете указать несколько IPv4-адресов или префиксов и удалить IPv4-адрес или префикс, нажав 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 вы 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 должно применяться к пакетам трафика. Если вы выключили использование технологии DPI при настройке основных параметров межсетевого экрана, правило автоматически выключается.

6. Нажмите на кнопку **Сохранить**.

Правило межсетевого экрана будет изменено и обновится в таблице.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Включение и выключение правила межсетевого экрана

По умолчанию ранее 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. Когда вы включаете или выключаете правило межсетевого экрана в шаблоне, это правило автоматически включается или выключается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Правила**.

   - Если вы хотите включить или выключить правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 верхней 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. Когда вы удаляете правило межсетевого экрана в шаблоне, это правило автоматически удаляется на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Правила**.

   - Если вы хотите удалить правило межсетевого экрана на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с наборами IP

Таблица наборов IP отображается в шаблоне межсетевого экрана и на устройстве CPE:

- Для отображения таблицы наборов IP в шаблоне межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN → Шаблоны межсетевого экрана**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Наборы IP**.

- Для отображения таблицы наборов IP на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Параметры межсетевого экрана → Наборы IP**.

Информация о наборах IP отображается в следующих столбцах таблицы:

- **Имя** – имя набора IP.

- **Совпадение** – относится ли набор IP к источнику или назначению пакетов трафика, а также содержит ли набор IP-адреса или подсети.

- **Записи** – IP-адреса или подсети, добавленные в набор.

Создание набора IP

Вы можете создать набор IP в шаблоне межсетевого экрана или на устройстве CPE. Когда вы создаете набор IP в шаблоне межсетевого экрана, этот набор IP автоматически создается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Наборы IP**.

   - Если вы хотите создать набор IP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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: 255 символов.

4. В раскрывающемся списке **Направление** выберите, относится ли набор IP к источнику или назначению пакетов трафика:

   - **Совпадает с источником** – набор содержит IP-адреса или подсети источника.

   - **Совпадает с назначением** – набор содержит IP-адреса или подсети назначения.

5. В раскрывающемся списке **Тип** выберите, содержит ли набор IP-адреса или подсети.

   - **Набор подсетей** – набор содержит подсети.
   - **Набор одиночных IP** – набор содержит IP-адреса.

6. Если в раскрывающемся списке **Тип** вы выбрали **Набор подсетей**, укажите подсеть, выполнив следующие действия:

   a. В блоке **Список записей** нажмите на кнопку **+ Добавить**.

   b. В отобразившемся поле введите IPv4-префикс. Вы можете указать диапазоны компонентов 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 подсеть, нажав рядом с ней на значок удаления ✕.

7. Если в раскрывающемся списке **Тип** вы выбрали **Набор одиночных IP**, укажите IP-адрес, выполнив следующие действия:

   a. В блоке **Список записей** нажмите на кнопку **+ Добавить**.

   b. В отобразившемся поле введите IPv4-адрес. Вы можете указать диапазоны компонентов 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-адрес, нажав рядом с ним на значок удаления ✕.

8. Нажмите на кнопку **Создать**.

   Набор IP будет создан и отобразится в таблице.

9. В верхней 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. Когда вы изменяете набор IP в шаблоне межсетевого экрана, этот набор автоматически изменяется на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Наборы IP**.
   - Если вы хотите изменить набор IP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 в поле **Имя** введите имя набора IP. Максимальная длина: 255 символов.

4. В раскрывающемся списке **Направление** выберите, относится ли набор IP к источнику или назначению пакетов трафика:

   - **Совпадает с источником** – набор содержит IP-адреса или подсети источника.
   - **Совпадает с назначением** – набор содержит IP-адреса или подсети назначения.

5. В раскрывающемся списке **Тип** выберите, содержит ли набор IP-адреса или подсети.

   - **Набор подсетей** – набор содержит подсети.
   - **Набор одиночных IP** – набор содержит IP-адреса.

6. Если в раскрывающемся списке **Тип** вы выбрали **Набор подсетей**, укажите подсеть, выполнив следующие действия:

   a. В блоке **Список записей** нажмите на кнопку **+ Добавить**.

   b. В отобразившемся поле введите IPv4-префикс. Вы можете указать диапазоны компонентов 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 подсеть, нажав рядом с ней на значок удаления ✕.

7. Если в раскрывающемся списке **Тип** вы выбрали **Набор одиночных IP**, укажите IP-адрес, выполнив следующие действия:

   a. В блоке **Список записей** нажмите на кнопку **+ Добавить**.

   b. В отобразившемся поле введите IPv4-адрес. Вы можете указать диапазоны компонентов 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-адрес, нажав рядом с ним на значок удаления ✕.

8. Нажмите на кнопку **Сохранить**.

   Набор IP будет изменен и обновится в таблице.

9. В верхней 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. Когда вы выключаете или включаете набор IP в шаблоне межсетевого экрана, этот набор автоматически выключается или включается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Наборы IP**.

   - Если вы хотите выключить или включить набор IP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 верхней 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. Когда вы удаляете набор IP в шаблоне межсетевого экрана, этот набор IP автоматически удаляется на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Наборы IP**.

   - Если вы хотите удалить набор IP на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с передачами

Таблица передач отображается в шаблоне межсетевого экрана или на устройстве CPE:

- Для отображения таблицы передач в шаблоне CPE вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны межсетевого экрана**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **Передачи между зонами**.
- Для отображения таблицы передач на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **Устройства CPE**, нажать на устройство, в отобразившейся области настройки выбрать вкладку **Параметры межсетевого экрана** → **Передачи между зонами**.

Информация о передачах отображается в следующих столбцах таблицы:

- **От** – исходящая зона.
- **До** – входящая зона.

Создание передачи

Вы можете создать передачу в шаблоне межсетевого экрана или на устройстве CPE. Когда вы создаете передачу в шаблоне межсетевого экрана, эта передача автоматически создается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Передачи между зонами**.
   - Если вы хотите создать передачу на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана** → **Передачи между зонами** и установите флажок **Переопределить**.

   Отобразится таблица передач.
2. Нажмите на кнопку **+ Передача**.
3. В открывшемся окне в раскрывающемся списке **От** выберите ранее созданную исходящую зону.
4. В раскрывающемся списке **До** выберите ранее созданную входящую зону.
5. Нажмите на кнопку **Создать**.

   Передача будет создана и отобразится в таблице.
6. В верхней 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. Когда вы удаляете передачу в шаблоне межсетевого экрана, эта передача автоматически удаляется на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **Передачи между зонами**.

   - Если вы хотите удалить передачу на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с DNAT-правилами

Таблица DNAT-правил отображается в шаблоне межсетевого экрана и на устройстве CPE:

- Для отображения 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 в отобразившейся области настройки выбрать вкладку **NAT → DNAT**.

- Для отображения таблицы DNAT-правил на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Параметры межсетевого экрана → NAT → DNAT**.

Информация о DNAT-правилах отображается в следующих столбцах таблицы:

- **Имя** – имя DNAT-правила.

- **Входящий** – критерии, согласно которым межсетевой экран должен применять DNAT-правило к пакетам трафика.

- **Перенаправленные** – 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. Когда вы создаете DNAT-правило в шаблоне межсетевого экрана, это правило автоматически создается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT → DNAT**.

   - Если вы хотите создать DNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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: 255 символов.

4. Укажите критерии, согласно которым межсетевой экран должен применять DNAT-правило к пакетам трафика, выполнив следующие действия:

   a. В раскрывающемся списке **Протокол** выберите протокол пакетов трафика, к которым межсетевой экран должен применять 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 должен применять DNAT-правило.

   c. Если вы хотите применять DNAT-правило только к пакетам трафика с указанной зоной источника, в раскрывающемся списке **Зона источника** выберите ранее созданную зону.

   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. 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.

5. Укажите, как DNAT-правило должно изменять пакеты трафика, выполнив следующие действия:

   a. В поле **IP назначения** введите новый IPv4-адрес или префикс назначения.

   b. В раскрывающемся списке **Зона назначения** выберите новую ранее созданную зону 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. Диапазон значений: от 1 до 65 535.

6. Нажмите на кнопку **Создать**.

   DNAT-правило будет создано и отобразится в таблице.

7. В верхней 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 правила в верхней части таблицы. По умолчанию DNAT-правила отображаются в таблице в порядке создания. Чем раньше правило было создано, тем выше оно отображается в таблице.

Вы можете настроить порядок применения DNAT-правил в шаблоне межсетевого экрана или на устройстве CPE. Когда вы настраиваете порядок применения DNAT-правил в шаблоне межсетевого экрана, этот порядок автоматически распространяется на все использующие шаблон устройства CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT → DNAT**.

   - Если вы хотите настроить порядок применения DNAT-правил на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → NAT → DNAT** и установите флажок **Переопределить**.

   Отобразится таблица DNAT-правил.

2. Настройте порядок применения DNAT-правил, нажимая рядом с ними на кнопки **UP** и **DOWN**.

3. В верхней 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. Когда вы изменяете DNAT-правило в шаблоне межсетевого экрана, это правило автоматически изменяется на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT → DNAT**.

   - Если вы хотите изменить DNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 в поле **Имя** введите имя DNAT-правила. Максимальная длина: 255 символов.

4. Укажите критерии, согласно которым межсетевой экран должен применять DNAT-правило к пакетам трафика, выполнив следующие действия:

   a. В раскрывающемся списке **Протокол** выберите протокол пакетов трафика, к которым межсетевой экран должен применять 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 должен применять DNAT-правило.

   c. Если вы хотите применять DNAT-правило только к пакетам трафика с указанной зоной источника, в раскрывающемся списке **Зона источника** выберите ранее созданную зону.

   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. 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.

5. Укажите, как DNAT-правило должно изменять пакеты трафика, выполнив следующие действия:

   a. В поле **IP назначения** введите новый IPv4-адрес или префикс назначения.

   b. В раскрывающемся списке **Зона назначения** выберите новую ранее созданную зону 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. Диапазон значений: от 1 до 65 535.

6. Нажмите на кнопку **Сохранить**.

DNAT-правило будет изменено и обновится в таблице.

7. В верхней 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. Когда вы выключаете или включаете DNAT-правило в шаблоне межсетевого экрана, это правило автоматически выключается или включается на всех использующих шаблон устройствах CPE.

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 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** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана** → **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 верхней 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. Когда вы удаляете DNAT-правило в шаблоне межсетевого экрана, это правило автоматически удаляется на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT** → **DNAT**.

   - Если вы хотите удалить DNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку

Параметры межсетевого экрана → **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 верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры шаблона межсетевого экрана или устройства CPE.

Работа с SNAT-правилами

Таблица SNAT-правил отображается в шаблоне межсетевого экрана и на устройстве CPE:

- Для отображения таблицы SNAT-правил в шаблоне межсетевого экрана вам нужно в меню перейти в раздел **SD-WAN** → **Шаблоны межсетевого экрана**, нажать на шаблон и в отобразившейся области настройки выбрать вкладку **NAT** → **SNAT**.

- Для отображения таблицы SNAT-правил на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN** → **Устройства CPE**, нажать на устройство, в отобразившейся области настройки выбрать вкладку **Параметры межсетевого экрана** → **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 должен применять SNAT-правило к пакетам трафика.

- **Действие** – действие, которое SNAT-правило должно выполнять с пакетами трафика.

Создание SNAT-правила

Вы можете создать SNAT-правило в шаблоне межсетевого экрана или на устройстве CPE. Когда вы создаете SNAT-правило в шаблоне межсетевого экрана, это правило автоматически создается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT** → **SNAT**.

   - Если вы хотите создать SNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана** → **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: 255 символов.

4. Укажите критерии, согласно которым межсетевой экран должен применять SNAT-правило к пакетам трафика, выполнив следующие действия:

   a. В раскрывающемся списке **Протокол** выберите протокол пакетов трафика, к которым межсетевой экран должен применять SNAT-правило:

      - **TCP**.
      - **UDP**.

   b. В раскрывающемся списке **Зона назначения** выберите ранее созданную зону назначения пакетов трафика, к которым межсетевой экран должен применять 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.

   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.

5. В раскрывающемся списке **Действие** выберите **SNAT**.

6. В поле **SNAT IP** введите новый IP-адрес или префикс источника, который SNAT-правило должно указывать для пакетов трафика.

7. Нажмите на кнопку **Создать**.

   SNAT-правило будет создано и отобразится в таблице.

8. В верхней 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 правила в верхней части таблицы. По умолчанию SNAT-правила отображаются в таблице в порядке создания. Чем раньше правило было создано, тем выше оно отображается в таблице.

Вы можете настроить порядок применения SNAT-правил в шаблоне межсетевого экрана или на устройстве CPE. Когда вы настраиваете порядок применения SNAT-правил в шаблоне межсетевого экрана, этот порядок автоматически распространяется на все использующие шаблон устройства CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT → SNAT**.

- Если вы хотите настроить порядок применения SNAT-правил на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана** → **NAT** → **SNAT** и установите флажок **Переопределить**.

Отобразится таблица SNAT-правил.

2. Настройте порядок применения SNAT-правил, нажимая рядом с ними на кнопки **UP** и **DOWN**.

3. В верхней 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. Когда вы изменяете SNAT-правило в шаблоне межсетевого экрана, это правило автоматически изменяется на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT** → **SNAT**.

   - Если вы хотите изменить SNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN** → **Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана** → **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 открывшемся окне в поле **Имя** введите имя SNAT-правила. Максимальная длина: 255 символов.

4. Укажите критерии, согласно которым межсетевой экран должен применять SNAT-правило к пакетам трафика, выполнив следующие действия:

   a. В раскрывающемся списке **Протокол** выберите протокол пакетов трафика, к которым межсетевой экран должен применять SNAT-правило:

      - **TCP**.

      - **UDP**.

   b. В раскрывающемся списке **Зона назначения** выберите ранее созданную зону назначения пакетов трафика, к которым межсетевой экран должен применять 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.

   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.

5. В раскрывающемся списке **Действие** выберите **SNAT**.

6. В поле **SNAT IP** введите новый IP-адрес или префикс источника, который SNAT-правило должно указывать для пакетов трафика.

7. Нажмите на кнопку **Сохранить**.

   SNAT-правило будет изменено и отобразится в таблице.

8. В верхней 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. Когда вы выключаете или включаете SNAT-правило в шаблоне межсетевого экрана, это правило автоматически выключается или включается на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT → SNAT**.

   - Если вы хотите выключить или включить SNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 верхней 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. Когда вы удаляете SNAT-правило в шаблоне межсетевого экрана, это правило автоматически удаляется на всех использующих шаблон устройствах CPE.

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 и в отобразившейся области настройки выберите вкладку **NAT → SNAT**.

- Если вы хотите удалить SNAT-правило на устройстве CPE, в меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Параметры межсетевого экрана → 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 верхней 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 между устройством CPE и подключенными к нему устройствами, а также к потере передаваемых пакетов трафика.

Чтобы изменить шаблон межсетевого экрана устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE, шаблон межсетевого экрана которого вы хотите изменить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет выбрана вкладка **Конфигурация**, на которой отображается основная информация об устройстве CPE. На этой вкладке также отображается таблица выполняемых оркестратором задач **Внеполосное управление**.

3. В раскрывающемся списке **Шаблон межсетевого экрана** выберите ранее созданный шаблон межсетевого экрана.

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

Управление сетевыми сервисами и виртуализация сетевых функций

Сетевые сервисы

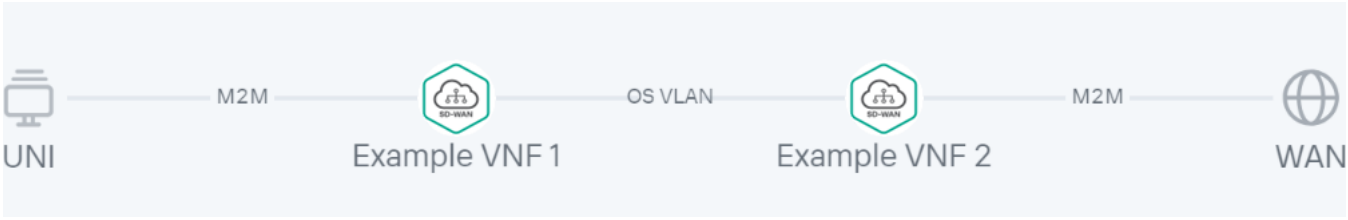
Сетевые сервисы передают трафик по сети и применяют к нему сетевые функции, например WAN-оптимизацию, шейпинг и защиту трафика. Каждый сетевой сервис имеет топологию, которую вы строите с помощью графического конструктора. Вы можете добавить в топологию компоненты и подключить их друг к другу.

Вам нужно построить топологию в шаблоне сетевого сервиса, после назначить этот шаблон тенанту. Вместе с шаблоном сетевого сервиса тенанту автоматически назначаются добавленные в топологию шаблона компоненты. Тенант может создавать и разворачивать сетевые сервисы, используя назначенные шаблоны, а также изменять уже развернутые сетевые сервисы.

При необходимости применить к трафику сетевые функции из разных сетевых сервисов, эти сетевые сервисы можно подключить к общему сетевому сервису.

С помощью сетевых сервисов вы можете развернуть экземпляры SD-WAN. Вам нужно войти в портал самообслуживания тенанта, для которого вы хотите развернуть экземпляр SD-WAN, создать сетевой сервис, добавить в топологию этого сетевого сервиса компоненты плоскости управления сетью и развернуть сетевой сервис. 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 объединения этих функций в сетевые сервисы.

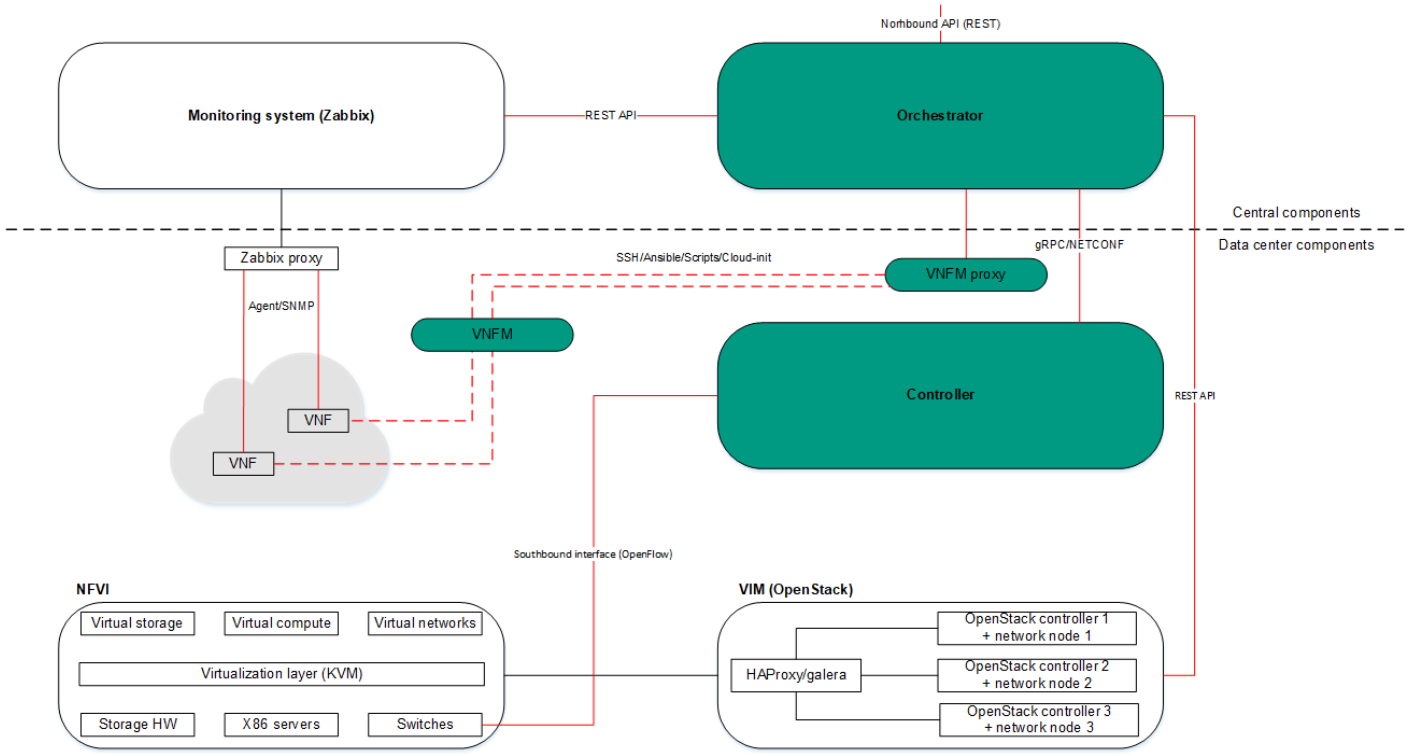
Вы можете использовать виртуальные сетевые функции (англ. Virtual Network Functions, далее также VNF) и физические сетевые функции (Physical Network Functions, далее также PNF). Разница между виртуальными и физическими сетевыми функциями заключается в том, что физические сетевые функции развертываются на специализированном оборудовании и не используют облачные ресурсы.

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 и физических сетевых функций и сообщает оркестратору о необходимости восстановить или масштабировать сетевую функцию.
- Инфраструктура NFV – состоит из физических ресурсов, таких как аппаратные хранилища, серверы и сетевые устройства.
- Контроллер SD-WAN

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 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 в формате YAML с параметрами сетевой функции.
- Директория /image – образы виртуальных машин в формате QCOW для развертывания виртуальной сетевой функции. Эта директория отсутствует в пакете PNF.
- Директория /scripts – скрипты для развертывания и управления сетевой функцией.
- Значок сетевой функции – файл в формате PNG. Необязательный компонент.
- PDF-файл с технической документацией или спецификацией виртуальной или физической сетевой функции. Необязательный компонент.

Вам нужно загрузить пакет VNF или PNF в веб-интерфейс оркестратора, чтобы добавить виртуальную или физическую сетевую функцию в топологию при работе с шаблоном сетевого сервиса или сетевым сервисом.

VNF-дескриптор

Вы можете указать следующие параметры и блоки в VNF-дескрипторе.

Значение	Тип	Обязательный	Описание
`name`	Параметр	✓	Имя виртуальной сетевой функции.
`description`	Параметр	✓	Краткое описание виртуальной сетевой функции.
`provider`	Параметр	✓	Поставщик виртуальной сетевой функции.
`version`	Параметр	✓	Версия виртуальной сетевой функции.
`description_file`	Параметр	–	Имя файла в формате PDF с технической документацией или спецификацией виртуальной сетевой функции. Вам нужно поместить файл в корневую директорию пакета VNF. Пользователи могут просмотреть и скачать файл.
`external_connections`	Блок	✓	Внешние точки подключения виртуальной сетевой функции. Вы можете настроить указанные внешние точки подключения виртуальной сетевой функции в веб-интерфейсе оркестратора.
`internal_connections`	Блок	–	Внутренние точки подключения VDU, входящих в состав виртуальной сетевой функции.
`virtual_links`	Блок	–	Виртуальные каналы для связи внутренних точек подключения. Вам нужно указать этот блок, если вы указали блок `internal_connections`.
`images`	Блок	✓	Образы дисков VDU. Вы можете развернуть несколько VDU с помощью одного образа диска VDU.
`configurations`	Блок	✓	Скрипты для выполнения действий на различных стадиях работы виртуальной сетевой функции, например при развертывании.
`flavours`	Блок	✓	Варианты развертывания виртуальной сетевой функции. Вы можете выбрать один из указанных вариантов развертывания в веб-интерфейсе оркестратора.
`scaling`	Блок	–	Параметры масштабирования виртуальной сетевой функции.
	Блок	–	Дополнительные вкладки, поля и

`user_configurations`			раскрывающиеся списки, которые должны быть добавлены в область настройки виртуальной сетевой функции.
`backups`	Блок	—	Задания резервного копирования виртуальной сетевой функции.

Пример VNF-дескриптора

```
name: "vGW backup"
description: "2.23.07.release.30"
provider: "Kaspersky"
version: "2.23.07.release.30"
external_connections:
- name: "WAN"
  description: "eth1"
  ip: "AUTO"
  mask: "AUTO"
- name: "LAN"
  description: "eth2"
  ip: "AUTO"
  mask: "AUTO"
images:
- name: "vgw"
  container_format: "BARE"
  disk_format: "QCOW2"
  type: "OPENSTACK"
  filename: "image.qcow2"
configurations:
- name: "config"
  filename: "config.yml"
  stage: "initialization"
  executor: "ansible"
  authentication: "password"
- name: "ztp"
  filename: "ztp.sh"
  stage: "none"
  executor: "/bin/sh"
  authentication: "password"
- name: "backup"
  filename: "backup.sh"
  stage: "none"
  executor: "/bin/sh"
  authentication: "password"
- name: "restore"
  filename: "restore.sh"
  stage: "none"
  executor: "/bin/sh"
  authentication: "password"
flavours:
- name: "Low"
  description: "1 vCPU, 512MB memory"
  position: 1
  management:
    vnc:
    - vdu_name: "vgw"
    ssh:
    - vdu_name: "vgw"
      def_user: "root"
      authentication: "key"
    web:
    - vdu_name: "vgw"
  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
    zabbix_template: "Template OS Linux"
    monitoring_type: "agent"
    ssh_port: 22
    configurations:
    - "config"
    - "ztp"
    backups:
    - "backup_config"
    def_user: "root"
    def_password: "p@ssw0rd"
    password_authentication: "yes"
    disks:
    - name: "default"
      order: 1
      type: "default"
      image: "vgw"
      storage_gb: 1
    cpu:
      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: "WAN"
    - name: "eth2"
      type: "data"
      description: "eth2"
      connection_point_ref: "LAN"
    auto_healing:
      triggers_set: "any"
      triggers:
      - name: "unreachable"
      action_set:
      - type: "reprovision"
- name: "Middle"
  description: "2 vCPU, 2048MB memory"
  position: 2
  management:
    vnc:
    - vdu_name: "vgw"
    ssh:
    - vdu_name: "vgw"
      def_user: "root"
      authentication: "key"
    web:
    - vdu_name: "vgw"
  vdus:
  - name: "vgw"
    password_rules:
      length: 12
      use_upper_case: true
      use_lower_case: true
      use_digits: true
      specific_symbols: .?$#@![]-{}
      specific_symbols_min_usage: 2
    zabbix_template: "Template OS Linux"
    monitoring_type: "agent"
    ssh_port: 22
    configurations:
    - "config"
    - "ztp"
    backups:
    - "backup_config"
    def_user: "root"
    def_password: "P@ssw0rd"
    password_authentication: "yes"
    disks:
    - name: "default"
      order: 1
      type: "default"
      image: "vgw"
      storage_gb: 1
    cpu:
      num_vpu: 2
    memory:
      total_memory_mb: 2048
    network_interfaces:
    - name: "Management"
      type: "management"
      description: "eth0"
    - name: "eth1"
      type: "data"
      description: "eth1"
      connection_point_ref: "WAN"
    - name: "eth2"
      type: "data"
      description: "eth2"
      connection_point_ref: "LAN"
    auto_healing:
      triggers_set: "any"
      triggers:
      - name: "unreachable"
      action_set:
      - type: "reprovision"
- name: "High"
  description: "4 vCPU, 4096MB memory"
  position: 2
  management:
    vnc:
    - vdu_name: "vgw"
    ssh:
    - vdu_name: "vgw"
      def_user: "root"
      authentication: "key"
    web:
    - vdu_name: "vgw"
  vdus:
  - name: "vgw"
    password_rules:
      length: 12
      use_upper_case: true
      use_lower_case: true
      use_digits: true
      specific_symbols: .?$#@![]-{}
      specific_symbols_min_usage: 2
    zabbix_template: "Template OS Linux"
    monitoring_type: "agent"
    ssh_port: 22
    configurations:
    - "config"
    - "ztp"
    backups:
    - "backup_config"
    def_user: "root"
    def_password: "P@ssw0rd"
    password_authentication: "yes"
```

```
    disks:
    - name: "default"
      order: 1
      type: "default"
      image: "vgw"
      storage_gb: 1
    cpu:
      num_vpu: 4
    memory:
      total_memory_mb: 4096
    network_interfaces:
    - name: "Management"
      type: "management"
      description: "eth0"
    - name: "eth1"
      type: "data"
      description: "eth1"
      connection_point_ref: "WAN"
    - name: "eth2"
      type: "data"
      description: "eth2"
      connection_point_ref: "LAN"
    - name: "Management"
      type: "management"
      description: "eth2"
    auto_healing:
      triggers_set: "any"
      triggers:
      - name: "unreachable"
      action_set:
      - type: "reprovision"
scaling:
  scale_up_status: "permit"
  scale_down_status: "permit"
user_configuration:
  tab:
  - name: "WAN"
    variables:
    - name: "gw_ip"
      description: "GW WAN IP"
      input_type: "input"
      required: true
      type: "string"
      default_value: "192.168.2.0"
      example: "192.168.2.0"
    - name: "gw_mask"
      description: "WAN Subnet mask GW1"
      input_type: "input"
      required: true
      type: "string"
      default_value: "255.255.255.0"
      example: "255.255.255.224"
    - name: "gw_gateway"
      description: "Deafult Gateway"
      input_type: "input"
      required: true
      type: "string"
      default_value: "192.168.0.1"
      example: "192.168.0.1"
  - name: "LAN"
    variables:
    - name: "lan_ip"
      description: "IP"
      input_type: "input"
      required: true
      type: "string"
      default_value: "192.168.0.1"
      example: "192.168.0.1"
    - name: "lan_mask"
      description: "Mask "
      input_type: "input"
      required: true
      type: "string"
      default_value: "255.255.255.0"
      example: "255.255.255.0"
backups:
- name: "backup_config"
  description: "Backup /etc/config"
  backup:
    path: "/root/config.tgz"
    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"
```

Блок external_connections

В блоке `external_connections` вы можете указать имена внешних точек подключения с помощью следующего параметра:

`- name`

Для каждой внешней точки подключения можно указать следующие параметры.

Значение	Обязательный	Описание
`description`	✓	Краткое описание внешней точки подключения.
`ip`	✓	IP-адрес внешней точки подключения виртуальной сетевой функции.
`mask`	✓	Маска подсети внешней точки подключения виртуальной сетевой функции.
`gw`	–	IP-адрес шлюза внешней точки подключения виртуальной сетевой функции.
`dns`	–	IP-адрес DNS-сервера внешней точки подключения виртуальной сетевой функции.
`group`	–	Группа, к которой относится внешняя точка подключения виртуальной сетевой функции. Обязательный параметр, если несколько VDU в составе виртуальной сетевой функции используют одну внешнюю точку подключения.

Для параметров `ip`, `mask`, `gw` и `dns` можно указать следующие значения:

- Ввести значение вручную – IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта и его невозможно изменить.
- `AUTO` – IP-адрес назначается автоматически с помощью внешнего DHCP-сервера или скриптов. Скрипты можно указать в блоке `configurations`.
- `MANUAL` – вам нужно указать IP-адрес вручную.

Пример блока external_connections

```
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"
```

Блок internal_connections

В блоке `internal_connections` вы можете указать имена внутренних точек подключения с помощью следующего параметра:

`- name`

Для каждой внутренней точки подключения можно указать следующие параметры.

Значение	Обязательный	Описание

description	✓	Краткое описание внутренней точки подключения.
virtual_link_name	✓	Имя виртуального канала внутренней точки подключения. Виртуальные каналы можно указать в блоке virtual_links.
ip	✓	IP-адрес внутренней точки подключения.
mask	✓	Маска подсети внутренней точки подключения.
gw	—	IP-адрес шлюза внутренней точки подключения.
dns	—	IP-адрес DNS-сервера внутренней точки подключения.
group	—	Группа, к которой относится внутренняя точка подключения. Обязательный параметр, если несколько VDU в составе виртуальной сетевой функции используют одну внутреннюю точку подключения.

Для параметров ip, mask, gw и dns можно указать следующие значения:

- Ввести значение вручную – IP-адрес назначается с помощью DHCP через резервирование по MAC-адресу OpenStack-порта и его невозможно изменить.
- AUTO – IP-адрес назначается автоматически с помощью внешнего DHCP-сервера или скриптов. Скрипты можно указать в блоке configurations.

Пример блока internal_connections

```
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"
```

Блок virtual_links

В блоке virtual_links вы можете указать имена виртуальных каналов с помощью следующего параметра:

- name

Для каждого виртуального канала можно указать следующие параметры:

- cidr

  IPv4-префикс виртуального канала.

- ip_version

  Версия IP-адресов в подсети. Возможные значения: v4 и v6.

Все параметры – обязательные.

Пример блока virtual_links

```
virtual_link:
- name: "int_link"
  cidr: 203.0.113.0/24
  ip_version: "v4"
```

Блок images

В блоке `images` вы можете указать имена образов дисков VDU с помощью следующего параметра:

`- name`

Для каждого образа диска VDU можно указать следующие параметры:

- `container_format`

  Формат контейнера для образа диска VDU.

- `disk_format`

  Формат образа диска VDU.

- `type`

  Тип VIM, например OpenStack.

- `file_name`

  Имя файла образа диска VDU. Вам нужно поместить образ диска VDU в директорию /image пакета VNF.

Все параметры – обязательные.

Пример блока images

```
images:
- name: "VDU_img"
  container_format: "BARE"
  disk_format: "QCOW2"
  type: "OPENSTACK"
  filename: "VDU_img.qcow2"
```

Блок configurations

В блоке `configurations` вы можете указать имена скриптов с помощью следующего параметра:

`- name`

Для каждого скрипта можно указать следующие параметры.

Значение	Обязательный	Описание
`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

		должен быть запущен. Возможные значения: • `initialization` – запустить скрипт при развертывании виртуальной сетевой функции. • `termination` – запустить скрипт при удалении виртуальной сетевой функции. • `none` – запустить скрипт при изменении значения в поле или раскрывающемся списке в области настройки виртуальной сетевой функции. Поля и раскрывающиеся списки можно указать в блоке `user_configurations`.
`executor`	✓	Интерпретатор. Возможные значения: • `ansible`; • `expect`; • `/bin/sh`; • `bin/bash`; • `cloud-init`. Вы можете ввести путь к пользовательскому исполнителю скрипта, например: `/user/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 этой 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 пользователя и паролю. Имя пользователя и пароль можно указать внутри блока `flavours` в блоке `vdus`.
`files_path`	–	Путь к файлам для запуска скриптов с помощью SSH. Вам нужно создать директорию внутри в директории /scripts пакета VNF и поместить в созданную директорию файлы. Файлы будут скопированы на VDU.
`config_drive`	–	Требуется ли использовать config-drive. Вы можете указать этот параметр, если для параметра `executor` вы указали значение `cloud_init`. Возможные значения: `true` или `false`.
`timeout`	–	Время ожидания выполнения скрипта в секундах. Если скрипт не выполняется по прошествии указанного времени, выполнение прерывается. Вы можете указать этот параметр, если для параметра `executor` вы указали путь к пользовательскому исполнителю скрипта. Отсчет времени начинается в момент запуска скрипта.

Пример блока configurations

```
configurations:
- name: "config"
  filename: "config.yml"
  stage: "initialization"
  executor: "ansible"
  authentication: "password"
  files_path: "SSH_scripts"
  config_drive: true
  timeout: 15
```

Блок flavours

В блоке `flavours` вы можете указать имена вариантов развертывания с помощью следующего параметра:

`- name`

Для каждого варианта развертывания можно указать следующие параметры и блоки.

Значение	Тип	Описание
`description`	Параметр	Краткое описание варианта развертывания.
`position`	Параметр	Порядковый номер варианта развертывания. Вариант развертывания с наименьшим порядковым номером имеет наименьшую производительность.
`affinity`	Блок	Группы VDU, которые должны быть размещены на одном хосте OpenStack. Мы рекомендуем разместить на одном хосте OpenStack VDU, требующие минимальных задержек при обмене информацией друг с другом.
`anti_affinity`	Блок	Группы VDU, которые должны быть размещены на разных хостах OpenStack. Мы рекомендуем развернуть на разных хостах OpenStack VDU, для которых может потребоваться вертикальное масштабирование или обеспечение отказоустойчивости.
`management`	Блок	Параметры консолей администрирования VDU.
`vdus`	Блок	Параметры VDU.

Все параметры и блоки – обязательные.

Блоки `affinity` и `anti_affinity`

Вы можете указать группы VDU с помощью следующего блока:

`groups`

В указанном блоке можно указать имена групп VDU с помощью следующего параметра:

`- name`

Для каждой группы VDU можно указать имена VDU с помощью следующего блока:

`vdu_name`

Пример блоков affinity и anti_affinity

```
affinity:
  groups:
  - name: "aff"
    vdu_name:
    - "VDU_1"
    - "VDU_2"
    - "VDU_3"
anti_affinity:
  groups:
  - name: "anti_aff"
    vdu_name:
    - "VDU_1"
    - "VDU_2"
    - "VDU_3"
```

Блок `management`

В блоке `management` вы можете указать следующие блоки:

- `vnc`

  Параметры управления VDU через VNC-консоль. Вы можете указать имена VDU с помощью следующего параметра:

  - `vdu_name`

- `ssh`

  Параметры управления VDU через SSH-консоль. Вы можете указать имена VDU с помощью следующего параметра:

  - `vdu_name`

  Для каждой VDU можно указать следующие параметры:

  - `def_user`

    Имя пользователя, от имени которого должна быть установлена SSH-сессия.

  - `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 этой функции. Вам нужно получить ключ с помощью скрипта. Скрипты можно указать в блоке `configurations`.

    - `password` – аутентифицировать VNFM в виртуальной сетевой функции по имени пользователя и паролю. Имя пользователя и пароль можно указать в блоке `vdus`.

  Все параметры – обязательные.

- `web`

  Параметры управления VDU через веб-консоль. Вы можете указать имена VDU с помощью следующего параметра:

  - `vdu_name`

  Для каждой VDU можно указать следующие параметры:

  - `protocol`

    Протокол подключения к веб-консоли. Возможные значения: `http` и `https`.

- `port`

  Порт подключения к веб-консоли. По умолчанию используется порт 80. Диапазон значений: от 1 до 65 536.

- `path`

  Путь к веб-консоли.

- `def_user`

  Имя пользователя для аутентификации в веб-консоли.

- `def_password`

  Пароль пользователя для аутентификации в веб-консоли.

Все параметры – необязательные.

Пример блока management

```
management:
  vnc:
  - vdu_name: "vgw"
  ssh:
  - vdu_name: "vgw"
    def_user: "root"
    authentication: "key"
  web:
  - vdu_name: "vgw"
```

Блок `vdus`

В блоке `vdus` вы можете указать имена VDU с помощью следующего параметра:

`- name`

Для каждой VDU можно указать следующие параметры и блоки.

Значение	Тип	Обязательный	Описание
`password_rules`	Блок	–	Требования к паролю VDU. Вы можете указать следующие параметры: • `length` Минимальная длина пароля. • `use_upper_case` Должны ли пользователи использовать прописные символы в пароле. Возможные значения: `true` или `false`. • `use_lower_case` Должны ли пользователи использовать строчные символы в пароле. Возможные значения: `true` или `false`. • `use_digits` Должны ли пользователи использовать цифры в пароле. Возможные значения: `true` или `false`.

			• `specific_symbols` Специальные символы, которые пользователи должны использовать в пароле, например $ и @. • `specific_symbols_min_usage` Минимальное количество специальных символов в пароле. Все параметры – необязательные.
`check_connection_mode`	Параметр	–	Тип проверки доступности VDU при развертывании. Возможные значения: `ssh` и `none`. По умолчанию используется SSH-проверка.
`zabbix_template`	Параметр	✓	Шаблон для создания на Zabbix-сервере хоста, соответствующего виртуальной сетевой функции.
`monitoring_type`	Параметр	✓	Тип мониторинга виртуальной сетевой функции. Возможные значения: • `agent` – мониторинг с помощью Zabbix-агента. • `snmp` – мониторинг с помощью протокола SNMP.
`ssh_port`	Параметр	–	Номер порта для установки SSH-сессии.
`configurations`	Блок	✓	Имена скриптов, которые должны быть запущены на VDU. Скрипты можно указать в блоке `configurations`.
`backups`	Блок	–	Имена заданий резервного копирования, которые должны быть использованы на VDU. Задания резервного копирования можно указать в блоке `backups`.
`def_user`	Параметр	–	Имя пользователя для аутентификации VNFM в виртуальной сетевой функции.
`def_password`	Параметр	–	Пароль для аутентификации VNFM в виртуальной сетевой функции.
`password_authentication`	Параметр	–	Разрешена ли аутентификация VNFM в виртуальной сетевой функции по паролю. Возможные значения: `yes` и `no`.
`disks`	Блок	✓	Имена виртуальных дисков VDU. Вы можете указать имена с помощью следующего параметра: `- name` Для каждого виртуального диска VDU можно указать следующие параметры: • `order` Порядок подключения виртуального диска VDU. Обязательный параметр.

			• `type` Тип эфемерного диска OpenStack. Обязательный параметр. • `image` Имя образа виртуального диска VDU. Образы виртуального диска VDU можно указать в блоке `images`. Необязательный параметр, если вы создаете пустой диск VDU. • `storage_db` Размер виртуального диска VDU в ГБ. Обязательный параметр.

`cpu`	Блок	✓	Параметры процессора VDU. Вы можете указать следующие параметры:
			• `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`
			Требуется ли использовать привязку 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.
			
			Все параметры – обязательные.

`memory`	Блок	✓	Параметры оперативной памяти VDU. Вы можете указать следующие параметры: • `total_memory_mb` Количество оперативной памяти VDU в МБ. • `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`. Все параметры – обязательные.
`network_interfaces`	Блок	✓	Параметры сетевых интерфейсов. Вы можете указать имена сетевых интерфейсов с помощью следующего параметра: `- name` Для каждого сетевого интерфейса можно указать следующие параметры: • `type` Тип сетевого интерфейса. Обязательный параметр. Возможные значения: • `data` – сетевой интерфейс для передачи данных. • `management` – управляющий сетевой интерфейс, который ссылается на сетевой порт. • `description` Краткое описание сетевого интерфейса. Обязательный параметр. • `connection_point_ref` Имена внешних точек подключения управляющего сетевого интерфейса. Обязательный параметр. Внешние точки подключения можно указать в блоке `exernal_connections`. • `port_security` Требуется ли включить функцию Port security. Необязательный параметр. Возможные значения: `disabled` и `enabled`.

			При необходимости указать vNIC-тип сетевого интерфейса вам нужно указать следующий блок:
			
			`properties`
			
			В указанном блоке можно указать vNIC-тип с помощью следующего параметра:
			
			`vnic_type`
			
			Возможные значения:
			
			• `virtio`;
			
			• `direct`;
			
			• `macvtap`;
			
			• `vhost`.

`auto_healing`	Блок	✓	Параметры автоматического восстановления VDU. Вы можете указать, какие внешние триггеры должны сработать, чтобы началось автоматическое восстановление VDU, с помощью следующего параметра:
			
			`triggers_set`
			
			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.
			
			Вы можете указать внешние триггеры, которые должны сработать, чтобы началось автоматическое восстановление VDU, с помощью следующего блока:
			
			`triggers`
			
			В указанном блоке можно указать имена внешних триггеров с помощью следующего параметра:
			
			`- name`
			
			Возможные значения:
			
			• `unreachable`;
			
			• `scale_up`;

			• `scale_down`.
			
			Вы можете указать, какое действие должно быть выполнено при срабатывании внешнего триггера с помощью следующего блока:
			
			`action_set`
			В указанном блоке можно указать действие с помощью следующего параметра:
			`- type`
			Возможные значения:
			• `reprovision` – повторно развернуть VDU.
			• `reboot` – перезагрузить VDU.
			• `script` – запустить указанный скрипт. При указании этого значения вам нужно указать имя скрипта с помощью следующего параметра: `configuration_name_ref` Скрипты можно указать в блоке `configurations`.

`bootstrap_timeout`	Параметр	–	Время ожидания доступности по SSH при развертывании VDU в секундах. Если VDU не доступна по SSH по истечении указанного времени, происходит откат развертывания.

Пример блока vdus

```
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"
    - "ztp"
    backups:
    - "backup_config"
    def_user: "root"
    def_password: "P@ssw0rd"
    password_authentication: "yes"
    disks:
    - name: "default"
      order: 1
      type: "default"
      image: "vgw"
      storage_gb: 1
    cpu:
      smt: prefer
      cpu_pinning: dedicated
      num_vpu: 4
    memory:
      total_memory_mb: 4096
      page_size: small
    network_interfaces:
    - name: "eth1"
      type: "data"
      description: "eth1"
      connection_point_ref: "WAN"
    auto_healing:
      triggers_set: "any"
      triggers:
      - name: "unreachable"
      action_set:
      - type: "reprovision"
```

Блок scaling

В блоке `scaling` вы можете указать следующие параметры:

- `scale_in_status`

  Разрешено ли горизонтальное масштабирование до варианта развертывания с более низким порядковым номером. Возможные значения: `permit` и `deny`.

- `scale_out_status`

  Разрешено ли горизонтальное масштабирование до варианта развертывания с более высоким порядковым номером. Возможные значения: `permit` и `deny`.

- `scale_up_status`

  Разрешено ли вертикальное масштабирование до варианта развертывания с более низким порядковым номером. Возможные значения: `permit` и `deny`.

- `scale_down_status`

  Разрешено ли вертикальное масштабирование до варианта развертывания с более высоким порядковым номером. Возможные значения: `permit` и `deny`.

Все параметры – необязательные.

Пример блока scaling

```
scaling:
  scale_in_status: "permit"
  scale_out_status: "permit"
  scale_up_status: "permit"
  scale_down_status: "permit"
```

Блок user_configurations

Вы можете указать вкладки, которые должны быть добавлены в область настройки виртуальной сетевой функции с помощью следующего блока:

`tab`

В указанном блоке можно указать имена вкладок с помощью следующего параметра:

`- name`

Для каждой вкладки можно указать поля и раскрывающиеся списки с помощью следующего блока:

`variables`

В указанном блоке можно указать имена полей и раскрывающихся списков с помощью следующего параметра:

`- name`

Для каждого поля и раскрывающегося списка можно указать следующие параметры и блоки.

Значение	Тип	Обязательный	Описание
`description`	Параметр	✓	Краткое описание поля или раскрывающегося списка.
`input_type`	Параметр	✓	Требуется ли добавить поле или раскрывающийся список. Возможные значения: • `input` – поле. • `dropdown` – раскрывающийся список.
`default_value`	Параметр	–	Значение по умолчанию в поле. Вы можете указать этот параметр, если для параметра `input_type` вы указали значение `input`.
`values`	Блок	–	Значения, которые должны отображаться в раскрывающемся списке. Вы можете указать этот блок, если для параметра `input_type` вы указали значение `dropdown`. Вы можете указать значения с помощью следующего параметра: `- value`

			Если вы хотите сделать одно из указанных значений значением по умолчанию, вам нужно указать после него следующий параметр: `is_default: true`
`required`	Параметр	—	Является ли поле или раскрывающийся список обязательным. Возможные значения: `true` или `false`.
`type`	Параметр	—	Тип значения, которое может быть указано в поле или раскрывающемся списке, например: `string`
`example`	Параметр	—	Подсказка, которая должна отображаться при изменении значения в поле или раскрывающемся списке.
`update_configuration_name`	Блок	—	Имена скриптов, которые должны быть запущены при изменении значения в поле или раскрывающемся списке. Скрипты можно указать в блоке `configurations`.

Пример блока user_configuration

```
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"
```

Блок backups

В блоке `backups` вы можете указать имена заданий резервного копирования с помощью следующего параметра:

`- name`

Для каждого задания резервного копирования можно указать следующие параметры и блоки.

Значение	Тип	Описание
`description`	Параметр	Краткое описание задания резервного копирования.
`backup`	Блок	Параметры резервного копирования. Вы можете указать следующие

		параметры: • `path` Путь в директории виртуальной сетевой функции, в которой расположены файлы для резервного копирования. • `interval` Интервал 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 этой функции. Вам нужно получить ключ с помощью скрипта. Скрипты можно указать в блоке `configurations`. • `password` – аутентифицировать VNFM в виртуальной сетевой функции по имени пользователя и паролю. Имя пользователя и пароль можно указать внутри блока flavours в блоке `vdus`. • `configuration_name_ref` Имя скрипта, который должен быть запущен перед резервным копированием. Скрипты можно указать в блоке `configurations`.
`restore`	Блок	Параметры восстановления из резервной копии. Вы можете указать следующие параметры: • `path` Путь в директории виртуальной сетевой функции, в которую должны быть помещены 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 этой функции. Вам нужно получить ключ с помощью скрипта. Скрипты можно указать в блоке `configurations`. • `password` – аутентифицировать VNFM в виртуальной сетевой функции по имени пользователя и паролю. Имя пользователя и пароль можно указать внутри блока flavours в блоке `vdus`. • `configuration_name_ref` Имя скрипта, который должен быть запущен после восстановления резервной копии. Скрипты можно указать в блоке `configurations`.

Все параметры и блоки – обязательные.

Пример блока backups

```
backups:
- name: "backup_config"
  description: "Backup /etc/config"
  backup:
    path: "/root/config.tgz"
    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"
```

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. Выберите пакет VNF или PNF.

VNF или PNF будет загружена в веб-интерфейс оркестратора и отобразится в панели **Каталог**.

Работа с шаблонами сетевых сервисов

Список шаблонов сетевых сервисов отображается в портале администратора в разделе **Инфраструктура** в панели **Каталог** на вкладке **Шаблоны**. Перед началом работы с шаблонами сетевых сервисов вам нужно войти в портал администратора.

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 в топологию, выполнив следующие действия:

   a. Перетащите в графический конструктор компоненты с панели **Каталог**. В этой панели отображаются следующие компоненты:

- Шаблоны сетевого сервиса – когда вы добавляете шаблон сетевого сервиса в топологию, топология выстраивается в соответствии с шаблоном.

- Общие сетевые сервисы – вам нужно добавить общий сетевой сервис в топологию сетевых сервисов, которые вы хотите подключить к этому общему сетевому сервису. Вы можете указать краткое описание общего сетевого сервиса в топологии.

- Виртуальные и физические сетевые функции. Действия, которые вы можете выполнить с виртуальными и физическими сетевыми функциями в топологии, описаны в разделах Работа с виртуальными сетевыми функциями в топологии и Работа с физическими сетевыми функциями в топологии.

b. Перетащите в графический конструктор соединения со вкладки **Соединения**. На этой вкладке отображаются следующие соединения:

- **P2P** – транспортный сервис Point-to-Point (далее также P2P-сервис). Вы можете настроить P2P-сервис в топологии.

- **P2M** – транспортный сервис Point-to-Multipoint (далее также P2M-сервис). Вы можете настроить P2M-сервис в топологии.

- **M2M** – транспортный сервис Multipoint-to-Multipoint (далее также M2M-сервис). Вы можете настроить M2M-сервис в топологии.

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 в топологии.

- **OS vRouter** – виртуальный маршрутизатор L3. Вы можете настроить виртуальный маршрутизатор в топологии.

- **OS VLAN** – VLAN для передачи тегированного L2-трафика стандарта 802.1Q. Вы можете настроить VLAN в топологии.

- **OS VXLAN** – VXLAN для туннелирования. Вы можете настроить VXLAN в топологии.

- **OS flat** – плоская сеть для передачи нетегированного L2-трафика. Вы можете настроить плоскую сеть в топологии.

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 должны быть подключены к WAN.

Вы можете настроить UNI в топологии.

Компоненты будут добавлены в топологию и отобразятся в графическом конструкторе.

4. Подключите добавленные в топологию компоненты друг к другу, выполнив следующие действия:

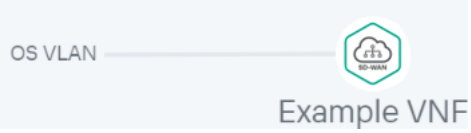
a. Нажмите на соединение, к которому вы хотите подключить компонент.

b. Нажмите на кнопку **Добавить leaf**, чтобы подключить к соединению компонент с ролью leaf. Если вы нажали на P2M-сервис, вы можете нажать на кнопку **Добавить root**, чтобы подключить к соединению

компонент с ролью root.

c. Нажмите на компонент, который вы хотите подключить к соединению. Если вы нажали на сетевую функцию или общий сетевой сервис, в открывшемся окне выберите порт для подключения.

К соединению будет подключен компонент, 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 UNI WAN является резервным для UNI.

6. Если вы хотите удалить компонент из топологии, выполните следующие действия:

a. Нажмите на компонент, который вы хотите удалить из топологии.

b. Нажмите на кнопку **Удалить**.

Компонент 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, снимите флажок **Описание**. По умолчанию флажок установлен.

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.

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. Добавьте компоненты в топологию, выполнив следующие действия:

   a. Перетащите в графический конструктор компоненты с панели **Каталог**. В этой панели отображаются следующие компоненты:

   - Шаблоны сетевого сервиса – когда вы добавляете шаблон сетевого сервиса в топологию, топология выстраивается в соответствии с шаблоном.
   - Общие сетевые сервисы – вам нужно добавить общий сетевой сервис в топологию сетевых сервисов, которые вы хотите подключить к этому общему сетевому сервису. Вы можете указать краткое описание общего сетевого сервиса в топологии.
   - Виртуальные и физические сетевые функции. Действия, которые вы можете выполнить с виртуальными и физическими сетевыми функциями в топологии, описаны в разделах Работа с виртуальными сетевыми функциями в топологии и Работа с физическими сетевыми функциями в топологии.

   b. Перетащите в графический конструктор соединения со вкладки **Соединения**. На этой вкладке отображаются следующие соединения:

   - **P2P** – транспортный сервис Point-to-Point (далее также P2P-сервис). Вы можете настроить P2P-сервис в топологии.
   - **P2M** – транспортный сервис Point-to-Multipoint (далее также P2M-сервис). Вы можете настроить P2M-сервис в топологии.
   - **M2M** – транспортный сервис Multipoint-to-Multipoint (далее также M2M-сервис). Вы можете настроить M2M-сервис в топологии.

   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 в топологии.

- **OS vRouter** – виртуальный маршрутизатор L3. Вы можете настроить виртуальный маршрутизатор в топологии.
- **OS VLAN** – VLAN для передачи тегированного L2-трафика стандарта 802.1Q. Вы можете настроить VLAN в топологии.
- **OS VXLAN** – VXLAN для туннелирования. Вы можете настроить VXLAN в топологии.
- **OS flat** – плоская сеть для передачи нетегированного L2-трафика. Вы можете настроить плоскую сеть в топологии.

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 должны быть подключены к WAN.

Вы можете настроить UNI в топологии.

Компоненты будут добавлены в топологию и отобразятся в графическом конструкторе.

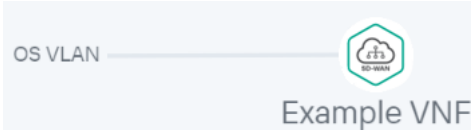
5. Подключите добавленные в топологию компоненты друг к другу, выполнив следующие действия:

a. Нажмите на соединение, к которому вы хотите подключить компонент.

b. Нажмите на кнопку **Добавить leaf**, чтобы подключить к соединению компонент с ролью leaf. Если вы нажали на P2M-сервис, вы можете нажать на кнопку **Добавить root**, чтобы подключить к соединению компонент с ролью root.

c. Нажмите на компонент, который вы хотите подключить к соединению. Если вы нажали на сетевую функцию или общий сетевой сервис, в открывшемся окне выберите порт для подключения.

К соединению будет подключен компонент, и в топологии между ними отобразится линия. Например, на рисунке ниже показана VLAN, к которой подключена виртуальная сетевая функция.



6. 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 UNI WAN является резервным для UNI.

7. Если вы хотите удалить компонент из топологии, выполните следующие действия:

   a. Нажмите на компонент, который вы хотите удалить из топологии.

   b. Нажмите на кнопку **Удалить**.

   Компонент будет удален из топологии и перестанет отображаться в графическом конструкторе.

8. Если вы хотите выровнять топологию по горизонтали, нажмите на кнопку **Выровнять**.

9. Если вы хотите, чтобы в топологии не отображались описания добавленных компонентов, снимите флажок **Описание**. По умолчанию флажок установлен.

10. В поле **Имя** введите имя шаблона сетевого сервиса.

11. В верхней части графического конструктора нажмите на кнопку **Сохранить**.

Шаблон сетевого сервиса будет изменен и обновится 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 на вкладке **Шаблоны**.

Работа с сетевыми сервисами

Список сетевых сервисов отображается в портале самообслуживания в разделе **Инфраструктура** в панели **Сетевые сервисы**. Перед началом работы с сетевыми сервисами вам нужно войти в портал самообслуживания тенанта.

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 в топологию, выполнив следующие действия:

   a. Перетащите в графический конструктор компоненты с панели **Каталог**. В этой панели отображаются следующие компоненты:

   - Шаблоны сетевого сервиса – когда вы добавляете шаблон сетевого сервиса в топологию, топология выстраивается в соответствии с шаблоном.
   - Общие сетевые сервисы – вам нужно добавить общий сетевой сервис в топологию сетевых сервисов, которые вы хотите подключить к этому общему сетевому сервису. Вы можете указать краткое описание общего сетевого сервиса в топологии.
   - Виртуальные и физические сетевые функции. Действия, которые вы можете выполнить с виртуальными и физическими сетевыми функциями в топологии, описаны в разделах Работа с виртуальными сетевыми функциями в топологии и Работа с физическими сетевыми функциями в топологии.

   b. Перетащите в графический конструктор соединения со вкладки **Соединения**. На этой вкладке отображаются следующие соединения:

   - **P2P** – транспортный сервис Point-to-Point (далее также P2P-сервис). Вы можете настроить P2P-сервис в топологии.
   - **P2M** – транспортный сервис Point-to-Multipoint (далее также P2M-сервис). Вы можете настроить P2M-сервис в топологии.
   - **M2M** – транспортный сервис Multipoint-to-Multipoint (далее также M2M-сервис). Вы можете настроить M2M-сервис в топологии.

   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 в топологии.
   - **OS vRouter** – виртуальный маршрутизатор L3. Вы можете настроить виртуальный маршрутизатор в топологии.

- **OS VLAN** – VLAN для передачи тегированного L2-трафика стандарта 802.1Q. Вы можете настроить VLAN в топологии.
- **OS VXLAN** – VXLAN для туннелирования. Вы можете настроить VXLAN в топологии.
- **OS flat** – плоская сеть для передачи нетегированного L2-трафика. Вы можете настроить плоскую сеть в топологии.

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 должны быть подключены к WAN.

Вы можете настроить UNI в топологии.

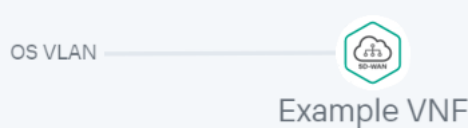
4. Подключите добавленные в топологию компоненты друг к другу, выполнив следующие действия:

a. Нажмите на соединение, к которому вы хотите подключить компонент.

b. Нажмите на кнопку **Добавить leaf**, чтобы подключить к соединению компонент с ролью leaf. Если вы нажали на P2M-сервис, вы можете нажать на кнопку **Добавить root**, чтобы подключить к соединению компонент с ролью root.

c. Нажмите на компонент, который вы хотите подключить к соединению. Если вы нажали на сетевую функцию или общий сетевой сервис, в открывшемся окне выберите порт для подключения.

К соединению будет подключен компонент, 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 UNI WAN является резервным для UNI.

6. Если вы хотите удалить компонент из топологии, выполните следующие действия:

   a. Нажмите на компонент, который вы хотите удалить из топологии.

   b. Нажмите на кнопку **Удалить**.

   Компонент 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, снимите флажок **Описание**. По умолчанию флажок установлен.

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. Добавьте компоненты в топологию, выполнив следующие действия:

   a. Перетащите в графический конструктор компоненты с панели **Каталог**. В этой панели отображаются следующие компоненты:

      - Шаблоны сетевого сервиса – когда вы добавляете шаблон сетевого сервиса в топологию, топология выстраивается в соответствии с шаблоном.
      - Общие сетевые сервисы – вам нужно добавить общий сетевой сервис в топологию сетевых сервисов, которые вы хотите подключить к этому общему сетевому сервису. Вы можете указать краткое описание общего сетевого сервиса в топологии.
      - Виртуальные и физические сетевые функции. Действия, которые вы можете выполнить с виртуальными и физическими сетевыми функциями в топологии, описаны в разделах Работа с виртуальными сетевыми функциями в топологии и Работа с физическими сетевыми функциями в топологии.

b. Перетащите в графический конструктор соединения со вкладки **Соединения**. На этой вкладке отображаются следующие соединения:

- **P2P** – транспортный сервис Point-to-Point (далее также P2P-сервис). Вы можете настроить P2P-сервис в топологии.
- **P2M** – транспортный сервис Point-to-Multipoint (далее также P2M-сервис). Вы можете настроить P2M-сервис в топологии.
- **M2M** – транспортный сервис Multipoint-to-Multipoint (далее также M2M-сервис). Вы можете настроить M2M-сервис в топологии.

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 в топологии.
- **OS vRouter** – виртуальный маршрутизатор L3. Вы можете настроить виртуальный маршрутизатор в топологии.
- **OS VLAN** – VLAN для передачи тегированного L2-трафика стандарта 802.1Q. Вы можете настроить VLAN в топологии.
- **OS VXLAN** – VXLAN для туннелирования. Вы можете настроить VXLAN в топологии.
- **OS flat** – плоская сеть для передачи нетегированного L2-трафика. Вы можете настроить плоскую сеть в топологии.

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 должны быть подключены к WAN.

Вы можете настроить UNI в топологии.

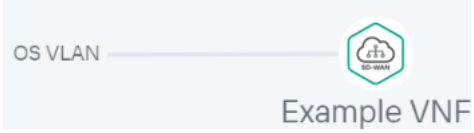
5. Подключите добавленные в топологию компоненты друг к другу, выполнив следующие действия:

a. Нажмите на соединение, к которому вы хотите подключить компонент.

b. Нажмите на кнопку **Добавить leaf**, чтобы подключить к соединению компонент с ролью leaf. Если вы нажали на P2M-сервис, вы можете нажать на кнопку **Добавить root**, чтобы подключить к соединению компонент с ролью root.

c. Нажмите на компонент, который вы хотите подключить к соединению. Если вы нажали на сетевую функцию или общий сетевой сервис, в открывшемся окне выберите порт для подключения.

К соединению будет подключен компонент, и в топологии между ними отобразится линия. Например, на рисунке ниже показана VLAN, к которой подключена виртуальная сетевая функция.



6. 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 UNI WAN является резервным для UNI.

7. Если вы хотите удалить компонент из топологии, выполните следующие действия:

   a. Нажмите на компонент, который вы хотите удалить из топологии.

   b. Нажмите на кнопку **Удалить**.

   Компонент будет удален из топологии и перестанет отображаться в графическом конструкторе.

8. Если вы хотите выровнять топологию по горизонтали, нажмите на кнопку **Выровнять**.

9. Если вы хотите, чтобы в топологии не отображались описания добавленных компонентов, снимите флажок **Описание**. По умолчанию флажок установлен.

10. В поле **Имя** введите имя сетевого сервиса.

11. 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 изменения.

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 согласованности (англ. consistency check) позволяет проверить, существуют ли компоненты, добавленные в топологию сетевого сервиса.

Чтобы проверить согласованность работы сетевого сервиса:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на значок настройки → **Проверить согласованность** рядом с сетевым сервисом, согласованность работы которого вы хотите проверить.

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

   Начнется проверка согласованности работы 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, 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.

Даже если автоматическое восстановление сетевого сервиса выключено, вы можете выполнить **автоматическое восстановление добавленных в топологию этого сетевого сервиса виртуальных сетевых функций или входящих в их 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 эта функция добавлена.

Чтобы автоматически восстановить виртуальную сетевую функцию или входящую в ее состав VDU:

1. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания. По умолчанию будет выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Если вы хотите выполнить автоматическое восстановление виртуальной сетевой функции, в верхней части области настройки нажмите на кнопку **Управление** → **Восстановление VNF**.

5. Если вы хотите выполнить автоматическое восстановление входящей в состав виртуальной сетевой функции VDU, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление** → **Восстановление VNF** рядом с VDU, автоматическое восстановление которой вы хотите выполнить.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Начнется автоматическое восстановление виртуальной сетевой функции или входящей в ее состав VDU.

Просмотр журнала работы сетевого сервиса

Чтобы просмотреть 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 просмотреть.

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**.

Указание краткого описания общего сетевого сервиса в топологии

Чтобы указать краткое описание общего сетевого сервиса в топологии 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.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки 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 в топологии

Для работы с виртуальной сетевой функцией вам нужно нажать на нее в топологии при выполнении следующих действий:

- при создании или изменении шаблона сетевого сервиса;
- при создании или изменении сетевого сервиса.

Параметры виртуальной сетевой функции отображаются 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.
  - **Диск** – количество назначенного VDU дискового пространства.
- **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 указываете в VNF-дескрипторе в блоке `user_configurations`.

Выбор варианта развертывания виртуальной сетевой функции

Вы можете указать варианты развертывания в VNF-дескрипторе в блоке `flavours`.

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. В топологии нажмите на виртуальную сетевую функцию, вариант развертывания которой вы хотите выбрать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет 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 VNF-дескрипторе в блоке `external_connections`.

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. В топологии нажмите на виртуальную сетевую функцию, внешние точки подключения которой вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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 должен назначить внешней точке подключения.
     b. В поле **Маска** введите маску подсети, которую DHCP должен назначить внешней точке подключения.
   - **AUTO** – автоматически назначить внешней точке подключения IPv4-префикс. Значение 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**. По умолчанию флажок снят.
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. В топологии нажмите на виртуальную сетевую функцию, основные параметры которой вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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. В топологии нажмите на виртуальную сетевую функцию, которую вы хотите разместить в центре обработки данных или на устройстве uCPE.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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 ранее созданного центра обработки данных. По мере ввода имени вам предлагается выбрать центр обработки данных в раскрывающемся списке.

b. В поле **VIM** введите имя ранее развернутого VIM для VNF. По мере ввода имени вам предлагается выбрать VIM в раскрывающемся списке.

- **uCPE** – разместить VNF на указанном устройстве uCPE. При выборе этого значения в поле **uCPE** введите имя устройства uCPE. По мере ввода имени вам предлагается выбрать uCPE в раскрывающемся списке.

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. Процессы, выполняемые на виртуальной сетевой функции или VDU, начинаются заново.

Чтобы остановить или запустить виртуальную сетевую функцию или входящую в ее состав VDU:

1. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. 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**.

5. Если вы хотите поставить на паузу или снять с паузы входящую в состав виртуальной сетевой функции VDU, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление** → **Питание** → **Поставить VDU на паузу** или **Снять паузу с VDU**.

6. 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 виртуальной 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 ожидания или активное состояние:

1. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Если вы хотите перевести виртуальную сетевую функцию в состояние ожидания или активное состояние, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** → **Приостановить VNF** или **Возобновить приостановленную VNF**.

5. Если вы хотите перевести входящую в состав виртуальной сетевой функции VDU в состояние ожидания или активное состояние, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление** → **Питание** → **Приостановить VDU** или **Возобновить приостановленную VDU** рядом с VDU, которую вы хотите перевести в состояние ожидания или активное состояние.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Виртуальная сетевая функция или входящая в ее состав VDU будет переведена в состояние ожидания 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**.

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 виртуальной 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 ожидания или активное состояние:

1. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Если вы хотите перевести виртуальную сетевую функцию в состояние ожидания или активное состояние, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** → **Приостановить VNF** или **Возобновить приостановленную VNF**.

5. Если вы хотите перевести входящую в состав виртуальной сетевой функции VDU в состояние ожидания или активное состояние, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление** → **Питание** → **Приостановить VDU** или **Возобновить приостановленную VDU** рядом с VDU, которую вы хотите перевести в состояние ожидания или активное состояние.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Виртуальная сетевая функция или входящая в ее состав VDU будет переведена в состояние ожидания или активное состояние.

Чтобы выполнить программную перезагрузку виртуальной сетевой функции или входящей в ее состав VDU:

1. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Если вы хотите выполнить программную перезагрузку виртуальной сетевой функции, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** →**Программная перезагрузка VNF**.

5. Если вы хотите выполнить программную перезагрузку входящей в состав виртуальной сетевой функции VDU, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление** → **Питание** → **Программная перезагрузка VDU** рядом с VDU, программную перезагрузку которой вы хотите выполнить.

6. 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. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Если вы хотите выполнить аппаратную перезагрузку виртуальной сетевой функции, в верхней части области настройки нажмите на кнопку **Управление** → **Питание** → **Аппаратная перезагрузка VNF**.

5. Если вы хотите выполнить аппаратную перезагрузку входящей в виртуальную сетевую функцию VDU, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление** → **Питание** → **Аппаратная перезагрузка VDU** рядом с VDU, аппаратную перезагрузку которой вы хотите выполнить.

6. 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 потери 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. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Если вы хотите повторно развернуть виртуальную сетевую функцию, в верхней части области настройки нажмите на кнопку **Управление** → **Повторно развернуть VNF**.

5. Если вы хотите повторно развернуть входящую в состав виртуальной сетевой функции VDU, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление** → **Восстановление VDU** рядом с VDU, которую вы хотите повторно развернуть.

6. 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 эта функция добавлена.

Чтобы автоматически восстановить виртуальную сетевую функцию или входящую в ее состав VDU:

1. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания.

4. Если вы хотите выполнить автоматическое восстановление виртуальной сетевой функции, в верхней части области настройки нажмите на кнопку **Управление → Восстановление VNF**.

5. Если вы хотите выполнить автоматическое восстановление входящей в состав виртуальной сетевой функции VDU, выполните следующие действия:

   a. Выберите вкладку **Управление VDU**.

      Отобразится таблица VDU.

   b. Нажмите на кнопку **Управление → Восстановление VNF** рядом с VDU, автоматическое восстановление которой вы хотите выполнить.

6. 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 отображения 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.
- **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. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию, в состав которой входит VDU.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию, в состав которой входит VDU.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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** → **Отменить** рядом с снимком состояния, с помощью которого вы хотите восстановить параметры VDU.

7. В открывшемся окне подтверждения нажмите на кнопку **Отменить**.

Параметры VDU будут установлены в соответствии с снимком состояния.

Изменение снимка состояния VDU

Чтобы изменить снимок состояния VDU:

1. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию, в состав которой входит VDU.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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 с снимком состояния VDU, который вы хотите изменить.

7. В поле **Имя** введите имя снимка состояния VDU.

8. В поле **Описание** введите краткое описание снимка состояния VDU.

9. 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. В портале самообслуживания в меню перейдите в раздел **Каталог**.

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на ранее развернутый сетевой сервис, в топологию которого добавлена виртуальная сетевая функция.

   Отобразится топология.

3. Нажмите на виртуальную сетевую функцию, в состав которой входит VDU.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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 с 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 в топологии

Для работы с физической сетевой функцией вам нужно нажать на нее в топологии при выполнении следующих действий:

- при создании или изменении шаблона сетевого сервиса;
- при создании или изменении сетевого сервиса.

Параметры физической сетевой функции отображаются 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 указываете в PNF-дескрипторе в блоке `user_configurations`.

Выбор варианта развертывания физической сетевой функции

Вы можете указать варианты развертывания в PNF-дескрипторе в блоке `flavours`.

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. В топологии нажмите на физическую сетевую функцию, вариант развертывания которой вы хотите выбрать.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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. В топологии нажмите на физическую сетевую функцию, основные параметры которой вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет 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 в облачной платформе OpenStack. 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 в топологии

Чтобы настроить P2P-сервис в топологии:

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 P2P-сервис, который вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃.

3. В поле **Имя** введите имя транспортного сервиса.

4. При необходимости в поле **Описание** введите краткое описание транспортного сервиса.

5. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры P2P-сервиса.

Настройка P2M-сервиса в топологии

Чтобы настроить P2M-сервис в топологии:

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 P2M-сервис, который вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃.

3. В поле **Имя** введите имя транспортного сервиса.

4. При необходимости в поле **Описание** введите краткое описание транспортного сервиса.

5. В поле **Точки подключения** введите максимальное количество точек подключения транспортного 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, хотите ли вы использовать Default Forwarding Interface (далее DFI), на который отправляется неизвестный unicast-трафик, в транспортном сервисе:

   - **Классический** – не использовать DFI. Значение по умолчанию.
   - **DFI с FIB на root и leafs** – использовать DFI на сервисном интерфейсе с ролью root. Количество сервисных интерфейсов с ролью leaf не ограничено. Для всех сервисных интерфейсов можно добавить резервные сервисные интерфейсы.
   - **DFI с FIB на leaf** – использовать DFI на сервисном интерфейсе с ролью root. Количество сервисных интерфейсов с ролью leaf не ограничено. Сервисные интерфейсы с ролью leaf должны находиться на одном устройстве CPE. Для всех сервисных интерфейсов можно добавить резервные сервисные интерфейсы.

     Резервные сервисные интерфейсы с ролью leaf должны находиться на одном устройстве CPE, отличном от устройства, на котором находятся основные сервисные интерфейсы.

7. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого вы хотите хранить записи в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. По умолчанию указано значение `300`.

8. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое вы хотите применять 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 таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отправляется на все добавленные в транспортный сервис сервисные интерфейсы, за исключением интерфейса, на который серия кадров пришла изначально. Значение по умолчанию.
   - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отбрасывается.

   > При наличии MAC-адреса назначения в таблице MAC-адресов 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. По умолчанию указано значение `100`.

10. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

    - **Flood** – трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Значение по умолчанию.
    - **Drop** – трафик с ранее 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**. По умолчанию выбрано значение **Выключить**.

    b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая должна назначать 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, из которого подсеть OpenStack должна назначать IP-адреса виртуальным сетевым функциям, выполнив следующие действия:

   1. В блоке **Пулы** нажмите на кнопку **+ Пул**.

   2. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

   Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав рядом с ним на кнопку **Удалить**.

e. Укажите DNS-сервер, который подсеть OpenStack должна назначать виртуальным сетевым функциям, выполнив следующие действия:

   1. В блоке **DNS** нажмите на кнопку **+ DNS**.

   2. 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 сервер, нажав рядом с ним на кнопку **Удалить**.

12. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры P2M-сервиса.

Настройка M2M-сервиса в топологии

Чтобы настроить M2M-сервис в топологии:

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 M2M-сервис, который вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃.

3. В поле **Имя** введите имя транспортного сервиса.

4. При необходимости в поле **Описание** введите краткое описание транспортного сервиса.

5. В поле **Точки подключения** введите максимальное количество точек подключения транспортного 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 вы хотите хранить записи в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. По умолчанию указано значение `300`.

7. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое вы хотите применять 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 таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отправляется на все добавленные в транспортный сервис сервисные интерфейсы, за исключением интерфейса, на который серия кадров пришла изначально. Значение по умолчанию.

- **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отбрасывается.

> При наличии MAC-адреса назначения в таблице MAC-адресов 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. По умолчанию указано значение `100`.

9. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

   - **Flood** – трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Значение по умолчанию.

   - **Drop** – трафик с ранее 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**. По умолчанию выбрано значение **Выключить**.

    b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая должна назначать 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, из которого подсеть OpenStack должна назначать IP-адреса виртуальным сетевым функциям, выполнив следующие действия:

       1. В блоке **Пулы** нажмите на кнопку **+ Пул**.

       2. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

       Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав рядом с ним на кнопку **Удалить**.

    e. Укажите DNS-сервер, который подсеть OpenStack должна назначать виртуальным сетевым функциям, выполнив следующие действия:

       1. В блоке **DNS** нажмите на кнопку **+ DNS**.

       2. 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 сервер, нажав рядом с ним на кнопку **Удалить**.

11. Если вы хотите использовать M2M-сервис для создания общего сетевого сервиса, установите флажок **Поделиться сетевым сервисом**. По умолчанию флажок снят.

12. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры M2M-сервиса.

Настройка общей сети (OS 2 SHARED) в топологии

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. В топологии нажмите на общую сеть, которую вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки 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) в топологии

Чтобы настроить виртуальный маршрутизатор в топологии:

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 виртуальный маршрутизатор, который вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки 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**. По умолчанию флажок снят.

6. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры виртуального маршрутизатора.

Настройка VLAN в топологии

Чтобы настроить VLAN в топологии:

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.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки 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**. По умолчанию выбрано значение **Выключить**.

   b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая должна назначать 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, из которого подсеть OpenStack должна назначать IP-адреса виртуальным сетевым функциям, выполнив следующие действия:

      1. В блоке **Пулы** нажмите на кнопку **+ Пул**.
      2. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

      Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав рядом с ним на кнопку **Удалить**.

   e. Укажите DNS-сервер, который подсеть OpenStack должна назначать виртуальным сетевым функциям, выполнив следующие действия:

      1. В блоке **DNS** нажмите на кнопку **+ DNS**.
      2. 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 сервер, нажав рядом с ним на кнопку **Удалить**.

6. Если вы хотите использовать сеть для создания общего сетевого сервиса, установите флажок **Поделиться сетью**. По умолчанию флажок снят.

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 в топологии

Чтобы настроить VXLAN в топологии:

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 VXLAN, которую вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки 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**. По умолчанию выбрано значение **Выключить**.

   b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая должна назначать 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, из которого подсеть OpenStack должна назначать IP-адреса виртуальным сетевым функциям, выполнив следующие действия:

      1. В блоке **Пулы** нажмите на кнопку **+ Пул**.
      2. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

      Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав рядом с ним на кнопку **Удалить**.

   e. Укажите DNS-сервер, который подсеть OpenStack должна назначать виртуальным сетевым функциям, выполнив следующие действия:

      1. В блоке **DNS** нажмите на кнопку **+ DNS**.
      2. 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 сервер, нажав рядом с ним на кнопку **Удалить**.

6. Если вы хотите использовать сеть для создания общего сетевого сервиса, установите флажок **Поделиться сетью**. По умолчанию флажок снят.

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 в топологии

Чтобы настроить плоскую 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. В топологии нажмите на плоскую сеть, которую вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки 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**. По умолчанию выбрано значение **Выключить**.

   b. В поле **CIDR** введите IPv4-префикс подсети OpenStack, которая должна назначать 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, из которого подсеть OpenStack должна назначать IP-адреса виртуальным сетевым функциям, выполнив следующие действия:

      1. В блоке **Пулы** нажмите на кнопку **+ Пул**.

      2. В отобразившихся полях введите начальное и конечное значение диапазона IP-адресов.

   Диапазон IP-адресов будет указан и отобразится в блоке **Пулы**. Вы можете указать несколько диапазонов IP-адресов и удалить диапазон, нажав рядом с ним на кнопку **Удалить**.

   e. Укажите DNS-сервер, который подсеть OpenStack должна назначать виртуальным сетевым функциям, выполнив следующие действия:

1. В блоке **DNS** нажмите на кнопку **+ DNS**.

2. 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 сервер, нажав рядом с ним на кнопку **Удалить**.

6. Если вы хотите использовать сеть для создания общего сетевого сервиса, установите флажок **Поделиться сетью**. По умолчанию флажок снят.

7. В верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры плоской сети.

Настройка UNI в топологии

Чтобы настроить UNI в топологии:

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 UNI, который вы хотите настроить.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки 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 и физических сетевых функций обеспечивается внешней системой мониторинга Zabbix. Вам нужно развернуть сервер Zabbix на одной из ваших площадок, либо подключить уже имеющийся сервер, а также развернуть серверы Zabbix-прокси.

Серверы Zabbix-прокси используются для получения результатов мониторинга на отдельных площадках и отправки этих результатов 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 добавляете VNF или PNF в топологию сетевого сервиса и развертываете сетевой сервис, на сервере Zabbix автоматически создается хост. Этот хост соответствует устройству CPE, VNF или PNF. Вы можете указать, в какие группы на сервере Zabbix должны помещаться хосты.

Поддерживается два способа мониторинга:

- Мониторинг 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 **Мониторинг**.

   Отобразятся параметры подключения к серверу Zabbix.

2. В поле **URL** введите веб-адрес Zabbix API. Оркестратор отправляет на этот веб-адресу HTTP-запросы для получения и отображения результатов мониторинга в виде графиков.

   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`.

3. 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.

4. В поле **Пароль** введите пароль пользователя для подключения к Zabbix API.

5. В раскрывающемся списке **Группировка по Zabbix** выберите способ группировки хостов устройств CPE, а также виртуальных и физических сетевых функций на сервере Zabbix:

   - **По указанным группам** – помещать хосты устройств CPE, а также виртуальных 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 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 и физических сетевых функций в автоматически созданные группы. Группы соответствуют тенантам, которым назначены устройства CPE, а также виртуальные и физические сетевые функции.

6. В поле **Синхронизация триггеров (сек.)** введите интервал в секундах для получения оркестратором уведомлений о возникших проблемах от сервера Zabbix. Диапазон значений: от 5 до 600. По умолчанию указано значение `600`.

7. Снизу от поля **Токен** нажмите на кнопку **Сгенерировать**, чтобы сгенерировать токен, который должны содержать API-запросы сервера Zabbix к оркестратору. Если API-запрос не содержит токен, оркестратор не принимает этот запрос. Безопасность также обеспечивается TLS-сертификатами.

   Вы можете ввести токен вручную, а также просмотреть его, нажав на значок просмотра 👁.

8. Если вы хотите проверить доступность сервера Zabbix, нажмите на кнопку **Проверить соединение**.

9. 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. В панели **Ресурсы** выберите ранее созданный домен и центр обработки данных, для которых 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 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. Когда вы настраиваете мониторинг в шаблоне CPE, указанные параметры распространяются на все использующие шаблон устройствам.

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 будет 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 просмотреть результаты мониторинга экземпляра SD-WAN, устройства CPE, а также виртуальной 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 и в отобразившейся области настройки выбрать вкладку **Мониторинг**.
- Для просмотра результатов мониторинга устройства CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Мониторинг**.
- Для просмотра результатов мониторинга виртуальной или физической сетевой функции вам нужно в портале самообслуживания, в меню перейти в раздел **Каталог**, в панели **Сетевые сервисы** нажать на ранее развернутый сетевой сервис, в топологию которого добавлена сетевая функция, нажать на виртуальную или физическую сетевую функцию и в отобразившейся области настройки выбрать вкладку **Мониторинг**.

Вы можете выбрать параметр, для которого отображаются результаты мониторинга, с помощью раскрывающегося списка в верхней части области настройки. Для отображения 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 эти проблемы классифицируются по уровням критичности. Таблица проблем отображается на устройстве CPE, а также на виртуальной и физической сетевой функции:

- Для просмотра таблицы проблем на устройстве CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки выбрать вкладку **Проблемы**.

- Для просмотра таблицы проблем на виртуальной или физической сетевой функции вам нужно в портале самообслуживания в меню перейти в раздел **Каталог**, в панели **Сетевые сервисы** нажать на ранее развернутый сетевой сервис, в топологию которого добавлена сетевая функция, нажать на виртуальную или физическую сетевую функцию и в отобразившейся области настройки выбрать вкладку **Проблемы**.

Информация о проблемах отображается в следующих столбцах таблицы:

- **Имя** – имя проблемы.
- **Уровень** – уровень критичности проблемы:
  - **Average**.
  - **Disaster**
  - **High**.
  - **Информация**.
  - **Не классифицировано**.
- **Время** – время возникновения проблемы.
- **Продолжительность** – продолжительность проблемы в секундах.

Просмотр состояния решения и его компонентов

Чтобы просмотреть 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 сессии** – активные пользовательские сеансы.

- **Ресурсы** – информация об использовании вычислительных ресурсов компонентами решения.
- **Сервисные запросы** – сервисные запросы.
- **Недоступные 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 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 которую обновляется отображаемая информация. Блоки можно перетаскивать 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 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 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 обновления информации в блоках будет изменен.

Просмотр журналов

Вы можете просмотреть журналы работы компонентов решения для осуществления технической поддержки. Kaspersky SD-WAN не отправляет журналы за пределы периметра информационной инфраструктуры вашей организации.

Чтобы просмотреть журналы:

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

   Откроется страница управления журналами.
2. В панели **Центры обработки данных** выберите ранее созданный центр обработки данных, к которому относятся компоненты решения.
3. В панели **Ресурсы** выберите компонент решения, журнал которого вы хотите просмотреть.

   Отобразится журнал. По умолчанию будет выбрана вкладка **Задачи**, на которой отображается таблица пользовательских задач. Информация о пользовательских задачах отображается в следующих столбцах таблицы:
   - **Действие задачи** – действие задачи.

- **Объект** – компонент решения, связанный с задачей.
- **СЗ** – ссылка на сервисный запрос, связанный с задачей.
- **ID объекта** – идентификатор компонента решения, связанного с задачей.
- **Имя объекта** – имя компонента решения, связанного с задачей.
- **Инициатор** – имя пользователя, выполнившего задачу.
- **IP инициатора** – IP-адрес пользователя, выполнившего задачу.
- **Время начала** – дата и время начала выполнения задачи.
- **Время окончания** – дата и время окончания выполнения задачи.

4. Если вы хотите просмотреть 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 просмотреть 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, создается соответствующий сервисный запрос.

Просмотр сервисных запросов

Вы можете просмотреть 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 и в отобразившейся области настройки выбрать вкладку **Сервисные запросы**.

  Отобразится таблица сервисных запросов.

- Для просмотра сервисных запросов устройства CPE вам нужно в меню перейти в раздел **SD-WAN → Устройства CPE**, нажать на устройство и в отобразившейся области настройки 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.
- **Действия** – действия, которые можно выполнить с сервисным запросом.

Вы можете открыть пошаговый журнал выполнения сервисного запроса, выполнив одно из следующих действий:

- Если вы хотите открыть пошаговый журнал выполнения сервисного запроса тенанта, нажмите на имя сервисного запроса.
- Если вы хотите открыть пошаговый журнал выполнения сервисного запроса экземпляра SD-WAN или устройства CPE, нажмите на идентификатор сервисного запроса.

Откроется пошаговый журнал выполнения сервисного запроса.

Журнал содержит информацию о шагах, на которых произошли ошибки, а также подробное описание ошибок.

Удаление сервисных запросов

Вы можете удалить сервисные запросы экземпляра SD-WAN и устройства CPE. 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 сервисные запросы**.

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 канала.
- Проблемы:
  - возникшие проблемы;
  - разрешенные проблемы.

Информация накапливается в течение пяти секунд перед отправкой уведомления. Например, если отключение порта приводит к отключению пяти туннелей, эту информацию необходимо накопить и отправить пользователю в одном уведомлении.

Администратору платформы нужно указать SMTP-сервер, который будет использоваться всеми тенантами для отправки уведомлений. В платформе администратора можно настроить отправку уведомлений о событиях и проблемах всех тенантов. В платформе самообслуживания можно настроить отправку уведомлений о событиях и проблемах отдельного тенанта.

Указание SMTP-сервера

Чтобы указать SMTP-сервер:

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

   По умолчанию будет выбрана вкладка **SMTP**, на которой отображаются параметры подключения к SMTP-серверу.

2. Установите флажок **Включить**, чтобы использовать SMTP-сервер. По умолчанию флажок снят.

3. В поле **SMTP-сервер** введите IP-адрес или доменное имя SMTP-сервера.

4. В поле **Порт SMTP-сервера** введите номер порта SMTP-сервера. Диапазон значений: от 0 до 65 535. По умолчанию указано значение `25`.

5. В поле **Адрес отправителя** введите адрес электронной почты, с которого SMTP-сервер должен отправлять уведомления пользователям.

6. 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. Значение по умолчанию.
   - **STARTTLS** – определить метод шифрования, после чего установить зашифрованное соединение.
   - **SMTPS** – изначально установить зашифрованное соединение.

7. Если вы хотите включить аутентификацию Kaspersky SD-WAN в SMTP-сервере, выполните следующие действия:

   a. Установите флажок **Аутентификация**. По умолчанию флажок снят.

   b. В поле **Имя пользователя** введите имя пользователя, которое Kaspersky SD-WAN должен использовать при аутентификации в SMTP-сервере. Максимальная длина: 64 символа.

   c. В поле **Пароль** введите пароль, который Kaspersky SD-WAN должен использовать при аутентификации в SMTP-сервере. Максимальная длина: 64 символа. Вы можете просмотреть введенный пароль, нажав на значок просмотра .

8. 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 должен отправить 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*.

9. Нажмите на кнопку **Применить**.

SMTP-сервер будет указан.

Настройка отправки уведомлений

Администратору платформы нужно указать SMTP-сервер, чтобы была возможна отправка уведомлений пользователю.

Чтобы настроить отправку уведомлений:

1. Перейдите к настройке отправки уведомлений пользователю одним из следующих способов:

- Если вы вошли в платформу администратора, в меню перейдите в раздел **Оповещения** и выберите вкладку **Предупреждение**.
- Если вы вошли в платформу самообслуживания, в меню перейдите в раздел **Оповещения**.

Отобразятся параметры отправки уведомлений.

2. Установите флажок **Включить**, чтобы отправлять уведомления пользователю. По умолчанию флажок снят.
3. В поле **Адресат** введите адрес электронной почты, на который вы хотите отправлять уведомления.
4. В поле **Тема** введите текст темы электронных писем с уведомлениями. Максимальная длина: 64 символа.
5. 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, которые используются, чтобы развернуть компоненты решения и поддерживать их работу. Вы можете выбрать уровень детализации этих журналов для мониторинга контейнеров и быстрого восстановления работы при возникновении сбоев.

Чтобы выбрать уровень детализации журналов Docker-контейнеров:

1. В нижней части меню нажмите на значок настройки → **Параметры журналов**.

   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.

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.

Мониторинг устройств CPE, VNF и PNF с помощью протокола SNMP

Вы можете использовать протокол SNMP для мониторинга устройств CPE, а также виртуальных и физических сетевых функций. Вам нужно установить SNMP-агента 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 агенты обмениваются запросами и уведомлениями. По умолчанию SNMP-агенты получают запросы от 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 агентов через порт 162. При этом 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 менеджера. При возникновении указанного вами события, например выключения устройства CPE или одного из его сетевых интерфейсов, SNMP-агент генерирует уведомление-ловушку и отправляет его менеджеру в виде UPD-сообщения. Ловушки позволяют автоматически информировать SNMP-менеджер о возникновении событий, не дожидаясь получения запроса.

- *Запрос на информирование* (англ. inform request) – это похожие на ловушки уведомления, которые отличаются тем, что требуют дополнительного подтверждения со стороны SNMP-менеджера. Когда SNMP-агент отправляет менеджеру запрос на информирование, этот агент ожидает получения подтверждения приема. Если SNMP-менеджер успешно принимает и обрабатывает запрос на информирование, он отправляет сообщение с подтверждением 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.

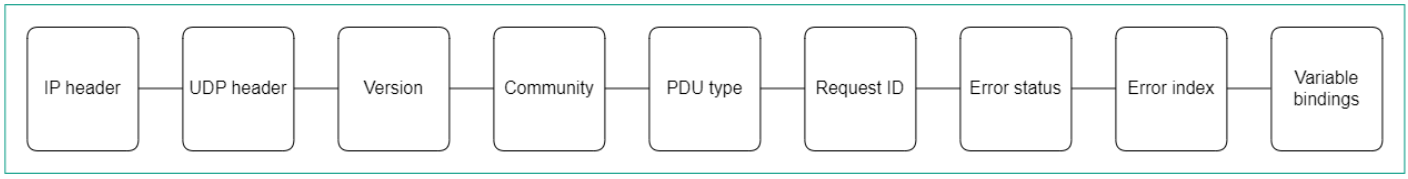


Схема единицы данных протокола SNMP

Для отображения таблицы уведомлений-ловушек вам нужно в меню перейти в раздел **Инфраструктура**, нажать на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключены компоненты для мониторинга, и в открывшемся меню настройки контроллера 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 должны отправлять менеджеру.
- **Описание** – краткое описание уведомления-ловушки.

Настройка подключения SNMP-менеджера к агентам

Вам нужно указать параметры подключения SNMP-менеджера к агентам, установленным на устройствах CPE, а также на виртуальных и физических сетевых функциях. Указанные параметры используются для всех SNMP-агентов.

Чтобы настроить подключение SNMP-менеджера к агентам:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключены компоненты для мониторинга.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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 используется как пароль, с помощью которого SNMP-менеджер подключается к агентам. По умолчанию указано значение `public`, которое предоставляет доступ только для чтения. Мы рекомендуем изменить значение по умолчанию на уникальную строку сообщества, чтобы обеспечить безопасность взаимодействия между SNMP-менеджером и агентами.

   Вам нужно указать одинаковую строку сообщества при настройке подключения SNMP-менеджера к 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 менеджеру.

Чтобы создать уведомление-ловушку:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключены компоненты для мониторинга.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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. По умолчанию указано значение `162`.

8. В поле **Сообщество** введите строку сообщества SNMP. Строка сообщества используется как пароль, с помощью которого SNMP-менеджер подключается к агентам. По умолчанию указано значение `public`, которое предоставляет доступ только для чтения. Мы рекомендуем изменить значение по умолчанию на уникальную строку сообщества, чтобы обеспечить безопасность взаимодействия между SNMP-менеджером и агентами.

   > Вам нужно указать одинаковую строку сообщества при настройке подключения SNMP-менеджера к 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 должны отправлять менеджеру:

   - Снимите флажок **Ловушка, когда интерфейс активен**, чтобы SNMP-агент не отправлял менеджеру уведомление-ловушку, когда один из портов компонента, на котором установлен агент, переходит в активное состояние.

   - Снимите флажок **Ловушка, когда интерфейс неактивен**, чтобы SNMP-агент не отправлял менеджеру уведомление-ловушку, когда один из портов компонента, на котором установлен агент, переходит в неактивное состояние.

   - Снимите флажок **Ловушка, когда оборудование активно**, чтобы SNMP-агент не отправлял менеджеру уведомление-ловушку, когда компонент, на котором установлен агент, переходит в активное состояние.

- Снимите флажок **Ловушка, когда оборудование неактивно**, чтобы SNMP-агент не отправлял менеджеру уведомление-ловушку, когда компонент, на котором установлен 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключены компоненты для мониторинга.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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 в поле **IP менеджера** введите IP-адрес или имя хоста SNMP-менеджера. Диапазон значений: от 1 до 255.
6. В поле **Порт менеджера** введите номер порта SNMP-менеджера. Диапазон значений: от 1 до 65 534. По умолчанию указано значение `162`.
7. В поле **Сообщество** введите строку сообщества SNMP. Строка сообщества используется как пароль, с помощью которого SNMP-менеджер подключается к агентам. По умолчанию указано значение `public`, которое предоставляет доступ только для чтения. Мы рекомендуем изменить значение по умолчанию на уникальную строку сообщества, чтобы обеспечить безопасность взаимодействия между SNMP-менеджером и агентами.

   Вам нужно указать одинаковую строку сообщества при настройке подключения SNMP-менеджера к агентам, а также при создании и изменении уведомлений-ловушек.

8. В поле **Разрешенные ловушки** нажмите на кнопку **Изменить** и снимите следующие флажки, чтобы выбрать, какие уведомления-ловушки SNMP-агенты не должны отправлять менеджеру:

   - Снимите флажок **Ловушка, когда интерфейс активен**, чтобы SNMP-агент не отправлял менеджеру уведомление-ловушку, когда один из сетевых интерфейсов устройства CPE или коммутатора, на котором установлен агент, переходит в активное состояние.

- Снимите флажок **Ловушка, когда интерфейс неактивен**, чтобы SNMP-агент не отправлял менеджеру уведомление-ловушку, когда один из сетевых интерфейсов устройства CPE или коммутатора, на котором установлен агент, переходит в неактивное состояние.

- Снимите флажок **Ловушка, когда оборудование активно**, чтобы SNMP-агент не отправлял менеджеру уведомление-ловушку, когда устройство CPE или коммутатор, на котором установлен агент, переходит в активное состояние.

- Снимите флажок **Ловушка, когда оборудование неактивно**, чтобы SNMP-агент не отправлял менеджеру уведомление-ловушку, когда устройство CPE или коммутатор, на котором установлен агент, переходит в неактивное состояние.

По умолчанию флажки установлены.

9. Нажмите на кнопку **Назад**, чтобы продолжить указывать параметры уведомления-ловушки.
10. В поле **Описание** введите краткое описание уведомления-ловушки.
11. 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером, к которому подключены компоненты для мониторинга.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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 канала

Чтобы настроить мониторинг канала:

1. Перейдите к настройке мониторинга канала одним из следующих способов:

   - В меню перейдите в раздел **SD-WAN → Устройства CPE**, нажмите на устройство, в отобразившейся области настройки выберите вкладку **Туннели** и нажмите на кнопку **Управление → Установить пороговые значения** рядом с каналом. На устройстве CPE отображаются только каналы, установленные с этого устройства.

   - В меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Меню конфигурации** рядом с контроллером, развернутым для экземпляра, в открывшемся меню перейдите в раздел **Туннели** и нажмите на кнопку **Управление → Установить пороговые значения** рядом с каналом.

   - В меню перейдите в раздел **Инфраструктура**, нажмите на кнопку **Управление → Меню конфигурации** рядом с контроллером, развернутым для экземпляра, в открывшемся меню перейдите в раздел **Топология**, нажмите на канал и в открывшемся окне нажмите на кнопку **Установить пороговые значения**.

2. Установите флажок **Включить мониторинг пороговых значений туннеля**, чтобы включить мониторинг канала.

3. Если вы включили мониторинг канала, настройте пороговые значения мониторинга, выполнив следующие действия:

   a. Если вы хотите установить пороговые значения мониторинга по умолчанию, нажмите на кнопку **Параметры по умолчанию**.

   b. Если вы хотите использовать канал в последнюю очередь при маршрутизации трафика независимо от качества связи, установите флажок **Нежелательный**. По умолчанию флажок снят.

   c. В поле **Интервал обработки ошибок и степени использования (сек.)** введите интервал в секундах для измерения количества ошибок на канале и уровня его загруженности. Диапазон значений: от 1 до 300. По умолчанию указано значение `60`.

   d. Если вы хотите указать пороговое значение количества ошибок в секунду на канале, установите флажок **Включить мониторинг ошибок** и в поле **Уровень критических ошибок (ошибок/сек.)** введите пороговое значение. Диапазон значений: от 1 до 1 000 000. По умолчанию флажок снят, и в поле указано значение `1000`.

   e. Если вы хотите указать пороговое значение загруженности канала в процентах от скорости сервисного интерфейса, с которого установлен канал, установите флажок **Включить мониторинг использования** и в поле **Критический уровень использования туннеля (%)** введите пороговое значение. По умолчанию флажок снят, и в поле указано значение `95`.

   f. В поле **Интервал обработки задержки, джиттера и потери пакетов (сек.)** введите интервал в секундах для измерения показателей задержки, джиттера и потерь пакетов на канале. Диапазон значений: от 1 до 600. По умолчанию указано значение `30`.

   g. Если вы хотите указать пороговое значение времени задержки в миллисекундах при передаче трафика по каналу, установите флажок **Включить мониторинг задержек** и в поле **Критический уровень задержек (мс.)** введите пороговое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, и в поле указано значение `100`.

   h. Если вы хотите указать пороговое значение времени джиттера в миллисекундах при передаче трафика по каналу, установите флажок **Включить мониторинг джиттера** и в поле **Критический уровень джиттера (мс.)** введите пороговое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, и в поле указано значение `100`.

i. Если вы хотите указать пороговое значение процента потерь пакетов трафика на канале, установите флажок **Включить мониторинг потерь пакетов** и в поле **Критический уровень потерь пакетов (%)** введите пороговое значение. Диапазон значений: от 1 до 100. По умолчанию флажок снят, и в поле указано значение 2.

4. Сохраните параметры мониторинга канала одним из следующих способов:

   - Если вы хотите сохранить параметры мониторинга канала, нажмите на кнопку **Сохранить**.

   - Если вы хотите сохранить параметры мониторинга канала и указать эти параметры на аналогичном встречном канале, нажмите на кнопку **Сохранить для обоих туннелей**.

5. Если вы настроили мониторинг канала на устройстве CPE, в верхней части области настройки нажмите на кнопку **Сохранить**, чтобы сохранить параметры устройства.

Туннели, сегменты и транспортные пути

Соединение между устройствами CPE обеспечивается туннелями. Туннели являются однонаправленными, поэтому при соединении двух устройств или устройства и плоскости управления сетью требуется построить как входящий, так и исходящий туннель. Установленные между устройствами CPE туннели объединятся в топологию.

Понятие *туннель* напрямую связано с понятием *канал* (англ. link), так как в случае SD-WAN каналы формируются внутри туннелей. Туннельный интерфейс напрямую связывается с портом виртуального коммутатора на устройстве CPE с обеих сторон, за счет чего формируется канал. Таким образом, в Kaspersky SD-WAN туннели являются средством формирования каналов.

Совокупность туннелей, соединяющих два устройства CPE, является *сегментом*. Трафик может быть распределен по нескольким туннелям на устройстве CPE-отправителе в начале сегмента и передан устройству CPE-получателю в конце сегмента.

Маршруты, по которым трафик может быть передан в рамках одного сегмента, называются *транспортными путями*. Поддерживается использование следующих типов транспортных путей:

- **Auto-SPF** (Shortest-Path Forwarding) – автоматически рассчитываемый контроллером SD-WAN транспортный путь. Транспортные пути этого типа невозможно создать и удалить, а также изменить их параметры.

- **Manual-TE** (Traffic Engineering) – транспортный путь, созданный вручную. При создании транспортного пути этого типа вам нужно указать туннели, через которые транспортный путь будет проходить от устройства CPE в начале сегмента до устройства в конце сегмента.

- **Auto-TE** – автоматически рассчитываемый контроллером SD-WAN транспортный путь, учитывающий ограничения (англ. constraints), которые вы указываете при создании транспортных сервисов. Ограничениями могут быть значения показателей мониторинга на туннелях, например показатель уровня загрузки туннеля.

Один сегмент может содержать от 2 до 16 транспортных путей, и при передаче трафика по умолчанию выбирается наилучший транспортный путь с наименьшим значением параметра стоимости. Если наилучший транспортный путь недоступен для передачи трафика по техническим причинам, выбирается другой транспортный путь с приближенным значением параметра стоимости.

Резервирование каналов между устройствами CPE

Все доступные каналы между устройствами CPE, например интернет и LTE, используются одновременно для предотвращения перерывов связи.

Режим Active/Active

В этом режиме все интерфейсы SD-WAN с типом WAN устройств CPE находятся в активном состоянии и передают трафик пользователей.

Контроллер SD-WAN использует от 2 до 16 транспортных путей, чтобы равномерно распределить трафик по туннелям и предотвратить перегрузку туннелей и возникновение проблем с производительностью у пользователей. Поддерживается три типа балансировки:

- По потокам (англ. per flow) с учетом информации на уровнях L2–L4. Доступно два режима:

- Эквивалентная балансировка – потоки распределяются равномерно по транспортным путям.
- Неэквивалентная балансировка – потоки распределяются по транспортным путям пропорционально стоимости туннелей.

- По пакетам (англ. per packet) – пакеты распределяются пропорционально стоимости туннелей при передаче.
- Широковещательный (англ. broadcast) – пакеты передаются одновременно во все туннели для исключения потерь.

В режиме Active/Active устройство CPE остается доступным, пока сохраняется работоспособность хотя бы одного канала.

Режим Active/Standby

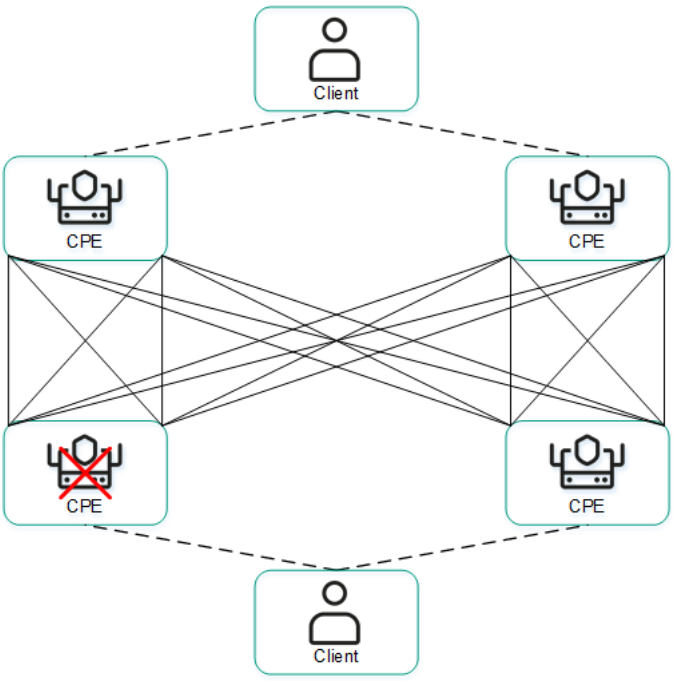
В этом режиме вам нужно выбрать основной и резервный транспортный путь для передачи трафика без использования балансировки. На устройство CPE заранее загружаются правила использования резервного интерфейса SD-WAN с типом WAN, если путь через основной интерфейс становится недоступным. При нарушении работы основного транспортного пути правила коммутации пакетов не переписываются, и устройство CPE отправляет их через резервный интерфейс.

Вы можете настроить резервирование на уровне транспортных сервисов. При создании транспортного сервиса вам нужно указать резервные сервисные интерфейсы (англ. reserve SI). Мы рекомендуем создавать основной и резервный сервисные интерфейсы на разных устройствах CPE. Трафик переключается на резервный сервисный интерфейс, если основной сервисный интерфейс недоступен.

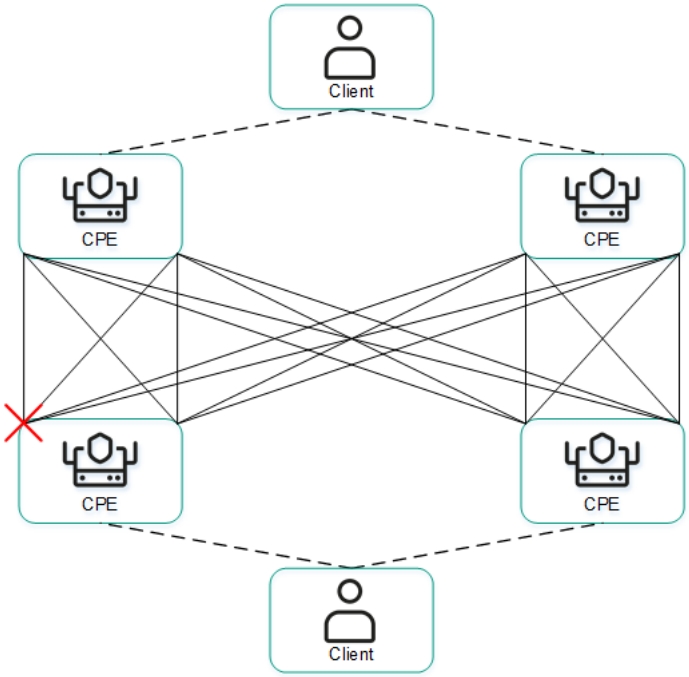
Решение поддерживает создание резервных сервисных интерфейсов для всех типов транспортных сервисов уровня L2.

На рисунках ниже представлены основные примеры перерывов связи между устройствами CPE:

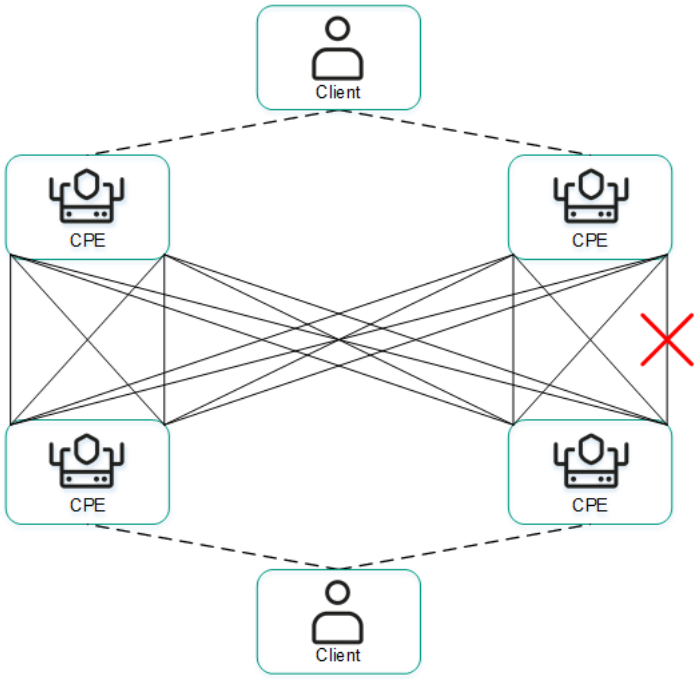
- Выход из строя одного из устройств CPE.



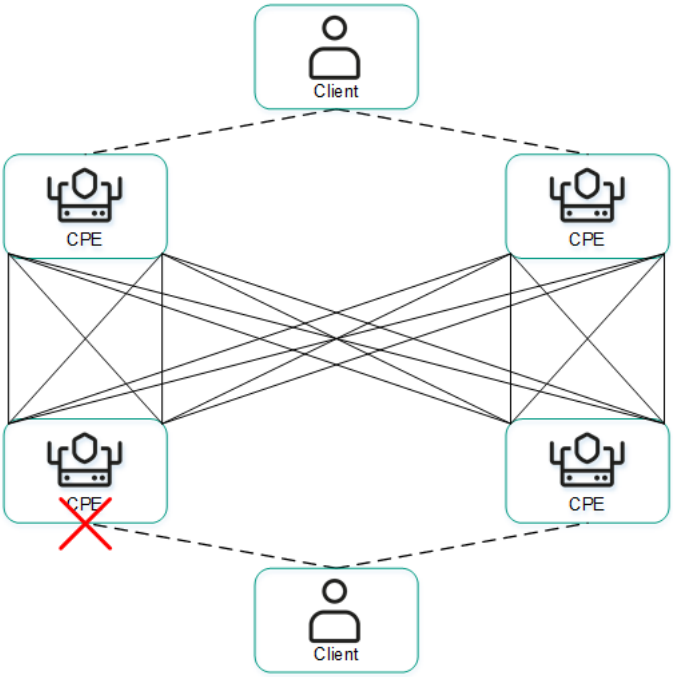
- Выход из строя SD-WAN интерфейса с типом WAN одного из устройств CPE.



- Выход из строя связности между двумя устройствами CPE.



- Выход из строя интерфейса SD-WAN с типом LAN одного из устройств CPE.



Настройка транспортных путей

Вы можете настроить транспортные пути в шаблоне CPE, на отдельном устройстве, а также в сегменте. Когда вы указываете параметры транспортных путей в шаблоне CPE или сегменте, эти параметры автоматически указываются на всех устройствах, использующих шаблон или входящих в сегмент. Для настройки транспортных путей используйте следующие инструкции:

- Настройка транспортных путей в шаблоне CPE.

Чтобы настроить транспортные пути в шаблоне CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на 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.

3. Выберите вкладку **Мультипутевая передача**.

   Отобразятся параметры транспортных путей.

4. В поле **Максимум транспортных путей** введите максимальное количество транспортных путей, поддерживаемое устройством CPE или сегментом. Диапазон значений: от 1 до 16. По умолчанию указано значение `8`.

5. В поле **Максимум Auto-SPF** введите максимальное количество транспортных путей типа Auto-SPF, поддерживаемое устройством CPE или сегментом. Транспортные пути типа Auto SPF автоматически рассчитываются контроллером SD-WAN. Диапазон значений: от 1 до 8. По умолчанию указано значение `2`.

6. В поле **Множитель разброса стоимости** введите коэффициент разброса стоимости, определяющий, во сколько раз больше может быть стоимость транспортного пути по сравнению с наилучшим транспортным путем, чтобы его можно было добавить в сегмент. Диапазон значений: от 1.0 до 10.0.

   По умолчанию указано значение `10`. Вы не можете ввести значение в этом поле, если установлен флажок **Балансировка трафика с учетом веса**.

7. При необходимости распределять трафик по транспортным путям примерно пропорционально значению атрибута веса (Path.weight) установите флажок **Балансировка трафика с учетом веса**. Когда флажок снят, трафик распределяется равномерно и значение атрибута веса для всех транспортных путей равно 1. По умолчанию флажок установлен.

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

- Настройка транспортных путей на отдельном устройстве CPE.

Чтобы настроить транспортные пути на отдельном устройстве CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Мультипутевая передача**.

   Отобразятся параметры транспортных путей.

4. В поле **Максимум транспортных путей** введите максимальное количество транспортных путей, поддерживаемое устройством CPE или сегментом. Диапазон значений: от 1 до 16. По умолчанию указано значение `8`.

5. В поле **Максимум Auto-SPF** введите максимальное количество транспортных путей типа Auto-SPF, поддерживаемое устройством CPE или сегментом. Транспортные пути типа Auto SPF автоматически рассчитываются контроллером SD-WAN. Диапазон значений: от 1 до 8. По умолчанию указано значение `2`.

6. В поле **Множитель разброса стоимости** введите коэффициент разброса стоимости, определяющий, во сколько раз больше может быть стоимость транспортного пути по сравнению с наилучшим транспортным путем, чтобы его можно было добавить в сегмент. Диапазон значений: от 1.0 до 10.0.

   По умолчанию указано значение `10`. Вы не можете ввести значение в этом поле, если установлен флажок **Балансировка трафика с учетом веса**.

7. При необходимости распределять трафик по транспортным путям примерно пропорционально значению атрибута веса (Path.weight) установите флажок **Балансировка трафика с учетом веса**. Когда флажок снят, трафик распределяется равномерно и значение атрибута веса для всех транспортных путей равно 1. По умолчанию флажок установлен.

8. Нажмите на кнопку **Применить**.

- Настройка транспортных путей в сегменте.

Чтобы настроить транспортные пути в сегменте:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сегменты**.

   Отобразится таблица сегментов.

4. Нажмите на кнопку **Управление** рядом с сегментом и в раскрывающемся списке выберите **Изменить**.

   Откроется окно, в котором отображаются параметры транспортных путей и таблица транспортных путей.

5. В поле **Максимум транспортных путей** введите максимальное количество транспортных путей, поддерживаемое устройством CPE или сегментом. Диапазон значений: от 1 до 16. По умолчанию указано значение `8`.

6. В поле **Максимум Auto-SPF** введите максимальное количество транспортных путей типа Auto-SPF, поддерживаемое устройством CPE или сегментом. Транспортные пути типа Auto SPF автоматически рассчитываются контроллером SD-WAN. Диапазон значений: от 1 до 8. По умолчанию указано значение `2`.

7. В поле **Множитель разброса стоимости** введите коэффициент разброса стоимости, определяющий, во сколько раз больше может быть стоимость транспортного пути по сравнению с наилучшим транспортным путем, чтобы его можно было добавить в сегмент. Диапазон значений: от 1.0 до 10.0.

   По умолчанию указано значение `10`. Вы не можете ввести значение в этом поле, если установлен флажок **Балансировка трафика с учетом веса**.

8. При необходимости распределять трафик по транспортным путям примерно пропорционально значению атрибута веса (Path.weight) установите флажок **Балансировка трафика с учетом веса**. Когда флажок снят, трафик распределяется равномерно и значение атрибута веса для всех транспортных путей равно 1. По умолчанию флажок установлен.

9. Нажмите на кнопку **Сохранить**.

Создание транспортного пути Manual-TE

При создании транспортного пути Manual-TE требуется вручную указать туннели, через которые он будет проходить от устройства CPE в начале сегмента до устройства в конце сегмента. Поддерживается создание двух типов таких транспортных путей:

- *Полностью определенные транспортные пути*, в которых указывается каждое устройство и интерфейс от начала до конца сегмента. В этом случае вы указываете каждый туннель, через который проходит транспортный путь.

- *Гибридные транспортные пути*, в которых указывается одно или несколько промежуточных устройств и при необходимости интерфейсы. В этом случае между не указанными узлами сети трафик передается автоматически (используется транспортный путь Auto-SPF).

Вы можете использовать ограничения, чтобы добавить транспортные пути Manual-TE в транспортные сервисы.

Примеры возможных транспортных путей Manual-TE:
В приведенных примерах для обозначения устройств CPE используется сокращение Sw (от англ. switch – коммутатор). После номера устройства через двоеточие указан номер интерфейса.
Полностью определенный транспортный путь: Sw1:3 → Sw2:1, Sw2:2 → Sw4:1, Sw4:5 → SwN:2.
Гибридный транспортный путь: Sw1 → Sw5, Sw5:3 → Sw4:3, Sw4 → SwN. В этом случае транспортный путь от Sw1 до SwN строится как транспортный путь Auto-SPF между Sw1 и Sw5, туннель Sw5:3 → Sw4:3 и транспортный путь Auto-SPF между Sw4 и SwN.

Чтобы создать транспортный путь Manual-TE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сегменты**.

   Отобразится таблица сегментов.

4. Нажмите на кнопку **Управление** рядом с сегментом и в раскрывающемся списке выберите **Изменить**.

   Откроется окно, в котором отображаются параметры и таблица транспортных путей.

5. Нажмите на кнопку **+ Путь Manual-TE**.

   Откроется окно, в котором отображаются параметры транспортного пути Manual-TE и таблица хопов.

6. В поле **Имя** ведите имя транспортного пути Manual-TE.

7. В поле **Максимум хопов** введите максимальное количество хопов в транспортном пути. Диапазон значений: от 1 до 8. По умолчанию указано значение 4.

8. В раскрывающемся списке **От** слева выберите начальное устройство CPE для хопа.

   Если в транспортном пути не создано ни одного хопа, в качестве начального устройства CPE можно выбрать только начальное устройство сегмента.

   Если в транспортном пути создан хотя бы один хоп, в качестве начального устройства CPE можно выбрать только конечное устройство последнего хопа.

9. При необходимости в раскрывающемся списке **Порт** слева выберите NNI (network-to-network interface) начального устройства CPE для хопа. По умолчанию выбрано значение **Автоматически** и интерфейс определяется автоматически.

10. В раскрывающемся списке **До** справа выберите конечное устройство CPE для хопа.

Если у начального устройства CPE для хопа в раскрывающемся списке **Порт** выбрано значение **Автоматически**, в качестве конечного устройства можно выбрать любое устройство в домене, за исключением тех, что используются в других хопах. При этом для конечного хопа в раскрывающемся списке **Порт** автоматически выбирается значение **Автоматически**. Таким образом, в хопе используется транспортный путь Auto-SPF.

Если у начального устройства CPE для хопа в раскрывающемся списке **Порт** выбран NNI, в качестве конечного устройства можно выбрать только устройство, до которого от NNI построен туннель. При этом для конечного устройства хопа в раскрывающемся списке **Порт** автоматически выбирается NNI, до которого построен туннель. Таким образом, в хопе используется указанный между двумя устройствами туннель.

11. При необходимости в раскрывающемся списке **Порт** справа выберите NNI (network-to-network interface) конечного устройства CPE для хопа. По умолчанию выбрано значение **Автоматически** и интерфейс определяется автоматически.

12. Нажмите на кнопку **Добавить**, чтобы добавить хоп в транспортный путь Manual-TE.

    Хоп будет добавлен и отобразится в таблице. В столбце **Сегменты** отобразится стоимость хопа, которая складывается из стоимости всех добавленных в него туннелей. Вы можете добавить несколько хопов, если не достигнуто их максимальное количество в транспортном пути.

13. Нажмите на кнопку **Создать**.

Будет выполнена проверка, что конечное устройство последнего хопа совпадает с конечным устройством сегмента, в котором создается транспортный путь Manual-TE. При успешной проверке транспортный путь Manual-TE будет создан и отобразится в таблице, а в столбце **Стоимость** отобразится стоимость транспортного пути, которая складывается из стоимости всех добавленных в него хопов.

Изменение транспортного пути Manual-TE

Чтобы изменить транспортный путь Manual-TE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сегменты**.

   Отобразится таблица сегментов.

4. Нажмите на кнопку **Управление** рядом с сегментом и в раскрывающемся списке выберите **Изменить**.

   Откроется окно, в котором отображаются параметры и таблица транспортных путей.

5. Нажмите на кнопку **Изменить** рядом с транспортным путем Manual-TE.

   Откроется окно, в котором отображаются параметры транспортного пути Manual-TE и таблица хопов.

6. Измените требуемые параметры. Описание параметров см. в инструкции по созданию транспортного пути Manual-TE.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры транспортного пути Manual-TE.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры сегмента.

Удаление хопа из транспортного пути Manual-TE

Удаленные из транспортного пути Manual-TE хопы невозможно восстановить.

Чтобы удалить хоп из транспортного пути Manual-TE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сегменты**.

   Отобразится таблица сегментов.

4. Нажмите на кнопку **Управление** рядом с сегментом и в раскрывающемся списке выберите **Изменить**.

   Откроется окно, в котором отображаются параметры и таблица транспортных путей.

5. Нажмите на кнопку **Изменить** рядом с транспортным путем Manual-TE.

   Откроется окно, в котором отображаются параметры транспортного пути Manual-TE и таблица хопов.

6. Нажмите на кнопку **Удалить** рядом с хопом.

   Хоп будет удален и перестанет отображаться в таблице.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры транспортного пути Manual-TE.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры сегмента.

Удаление транспортного пути Manual-TE

Удаленные транспортные пути Manual-TE невозможно восстановить.

Чтобы удалить транспортный путь Manual-TE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Сегменты**.

   Отобразится таблица сегментов.

4. Нажмите на кнопку **Управление** рядом с сегментом и в раскрывающемся списке выберите **Изменить**.

   Откроется окно, в котором отображаются параметры и таблица транспортных путей.

5. Нажмите на кнопку **Удалить** рядом с транспортным путем Manual-TE.

   Транспортный путь Manual-TE будет удален и перестанет отображаться в таблице.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры сегмента.

Указание стоимости туннеля

Вы можете указать стоимость отдельного туннеля. Туннели отображаются в общей таблице в разделе **Туннели**, в графической топологии в разделе **Топология**, а также в конфигурации устройств CPE на вкладке **Туннели**. В конфигурации устройства CPE отображаются только туннели, построенные с использованием этого устройства.

Для указания стоимости туннеля используйте следующие инструкции:

- Указание стоимости туннеля с помощью общей таблицы туннелей.

  Чтобы указать стоимость туннеля с помощью общей таблицы туннелей:

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

     Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

  2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

     Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

  3. Перейдите в раздел **Туннели**.

     Отобразится таблица туннелей.

  4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Указать стоимость**.

  5. В открывшемся окне установите флажок **Переопределить**, чтобы указать стоимость туннеля.

  6. В поле **Стоимость туннеля** введите стоимость туннеля.

  7. При необходимости автоматически назначить указанную стоимость аналогичному встречному туннелю установите флажок **Сохранить для обоих туннелей**.

  8. Нажмите на кнопку **Сохранить**.

- Указание стоимости туннеля с помощью графической топологии.

Чтобы указать стоимость туннеля с помощью графической топологии:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Топология**.

   Отобразится топология сети SD-WAN.

4. Нажмите на туннель и в открывшемся окне нажмите на кнопку **Указать стоимость**.

5. В открывшемся окне установите флажок **Переопределить**, чтобы указать стоимость туннеля.

6. В поле **Стоимость туннеля** введите стоимость туннеля.

7. При необходимости автоматически назначить указанную стоимость аналогичному встречному туннелю установите флажок **Сохранить для обоих туннелей**.

8. Нажмите на кнопку **Сохранить**.

- Указание стоимости туннеля в конфигурации устройства CPE.

Чтобы указать стоимость туннеля в конфигурации устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Указать стоимость**.

5. В открывшемся окне установите флажок **Переопределить**, чтобы указать стоимость туннеля.

6. В поле **Стоимость туннеля** введите стоимость туннеля.

7. При необходимости автоматически назначить указанную стоимость аналогичному встречному туннелю установите флажок **Сохранить для обоих туннелей**.

8. Нажмите на кнопку **Сохранить**.

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

Включение функции Dampening

Функция Dampening – это настраиваемый механизм, исключающий использование туннелей, состояние которых меняется слишком часто. При определении нестабильности учитываются изменения следующих состояний:

- UP/LIVE → DOWN/NOT-LIVE.
- DOWN/NOT-LIVE → UP/LIVE.
- UP/LIVE → UP/NOT-LIVE.
- UP/NOT-LIVE → UP/LIVE.

Состояния LIVE и NOT-LIVE используются для интеграции функции Dampening с протоколом Ethernet Connectivity Fault Management (CFM), который обнаруживает пропадание двухсторонней Ethernet-связности сегмента между соседними коммутаторами без перехода сервисного интерфейса в состояние DOWN (пропадание Rx-сигнала).

Функция Dampening применяется к обоим концам Ethernet-сегмента.

Функция выполняет следующие действия в рамках развернутой сети SD-WAN:

- обнаруживает частые изменения состояний сервисных интерфейсов;
- перемещает транспортные сервисы, проходящие через нестабильные сервисные интерфейсы, на резервные туннели;
- исключает сегменты, привязанные к сервисным интерфейсам, из расчета маршрутов для транспортных сервисов.

Когда функция Dampening включена, каждое изменение состояния сервисного интерфейса, через который построен туннель, увеличивает значение показателя Penalty. Если показатель Penalty достигает порогового значения за определенный промежуток времени, доступ к туннелю ограничивается (его стоимость повышается в 10 000 раз на определенный промежуток времени). Вы указываете значение каждого из этих параметров при включении функции. По умолчанию доступ к туннелю возобновляется, если в течение 10 минут не происходит ни одного изменения состояния сервисного интерфейса.

Вы можете включить функцию Dampening на отдельном туннеле. Туннели отображаются в общей таблице в разделе **Туннели**, в графической топологии в разделе **Топология**, а также в конфигурации устройств CPE на вкладке **Туннели**. В конфигурации устройства CPE отображаются только туннели, построенные с использованием этого устройства.

Для включения функции Dampening на туннеле используйте следующие инструкции:

- **Включение функции Dampening на туннеле с помощью общей таблицы туннелей**.

Чтобы включить функцию Dampening на туннеле с помощью общей таблицы туннелей:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Dampening**.

5. В открывшемся окне установите флажок **Включить**.

6. В поле **Максимальное время блокировки (мс.)** введите максимальное время в миллисекундах, в течение которого доступ к туннелю может быть ограничен. По истечении указанного времени все счетчики функции Dampening на туннеле сбрасываются. По умолчанию указано значение `600000`.

7. В поле **Штраф** введите число, которое требуется прибавлять к показателю Penalty при изменении состояния туннеля. По умолчанию указано значение `1`.

8. В поле **Порог блокировки** введите значение показателя Penalty, при котором доступ к туннелю ограничивается. По умолчанию указано значение `4`.

9. В поле **Интервал обновления (мс.)** введите время в миллисекундах, за которое показатель Penalty должен набрать значение в поле **Порог блокировки**, чтобы ограничить доступ к туннелю. По умолчанию указано значение `120000`.

10. При необходимости просмотреть статистику работы функции Dampening на туннеле нажмите на кнопку **Загрузить статистику**.

11. Нажмите на кнопку **Сохранить**.

- Включение функции Dampening на туннеле с помощью графической топологии.

Чтобы включить функцию Dampening на туннеле с помощью графической топологии:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Топология**.

   Отобразится топология сети SD-WAN.

4. Нажмите на туннель и в открывшемся окне нажмите на кнопку **Dampening**.

5. В открывшемся окне установите флажок **Включить**.

6. В поле **Максимальное время блокировки (мс.)** введите максимальное время в миллисекундах, в течение которого доступ к туннелю может быть ограничен. По истечении указанного времени все счетчики функции Dampening на туннеле сбрасываются. По умолчанию указано значение `600000`.

7. В поле **Штраф** введите число, которое требуется прибавлять к показателю Penalty при изменении состояния туннеля. По умолчанию указано значение `1`.

8. В поле **Порог блокировки** введите значение показателя Penalty, при котором доступ к туннелю ограничивается. По умолчанию указано значение `4`.

9. В поле **Интервал обновления (мс.)** введите время в миллисекундах, за которое показатель Penalty должен набрать значение в поле **Порог блокировки**, чтобы ограничить доступ к туннелю. По умолчанию указано значение `120000`.

10. При необходимости просмотреть статистику работы функции Dampening на туннеле нажмите на кнопку **Загрузить статистику**.

11. Нажмите на кнопку **Сохранить**.

- Включение функции Dampening на туннеле в конфигурации устройства CPE.

Чтобы включить функцию Dampening на туннеле в конфигурации устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Dampening**.

5. В открывшемся окне установите флажок **Включить**.

6. В поле **Максимальное время блокировки (мс.)** введите максимальное время в миллисекундах, в течение которого доступ к туннелю может быть ограничен. По истечении указанного времени все счетчики функции Dampening на туннеле сбрасываются. По умолчанию указано значение `600000`.

7. В поле **Штраф** введите число, которое требуется прибавлять к показателю Penalty при изменении состояния туннеля. По умолчанию указано значение `1`.

8. В поле **Порог блокировки** введите значение показателя Penalty, при котором доступ к туннелю ограничивается. По умолчанию указано значение `4`.

9. В поле **Интервал обновления (мс.)** введите время в миллисекундах, за которое показатель Penalty должен набрать значение в поле **Порог блокировки**, чтобы ограничить доступ к туннелю. По умолчанию указано значение `120000`.

10. При необходимости просмотреть статистику работы функции Dampening на туннеле нажмите на кнопку **Загрузить статистику**.

11. Нажмите на кнопку **Сохранить**.

12. 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 каналах, 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 на передающей стороне.

Мы рекомендуем использовать FEC на noisy links (или зашумленных каналах) для уменьшения коэффициента потери пакетов трафика и увеличения скорости TCP-соединений.

Передающее устройство CPE кодирует поток выходящих в туннель пакетов трафика и добавляет избыточные пакеты. Использование кодирования на передающей и принимающей сторонах может привести к задержкам, вызванным дополнительной обработкой данных. Степень избыточности вы можете настроить в свойствах контроллера SD-WAN или при включении функции FEC.

Принимающее устройство CPE буферизует принятые через туннель пакеты трафика и декодирует их, восстанавливая потерянные пакеты, если это возможно. Общая схема работы функции FEC представлена на рисунке ниже.

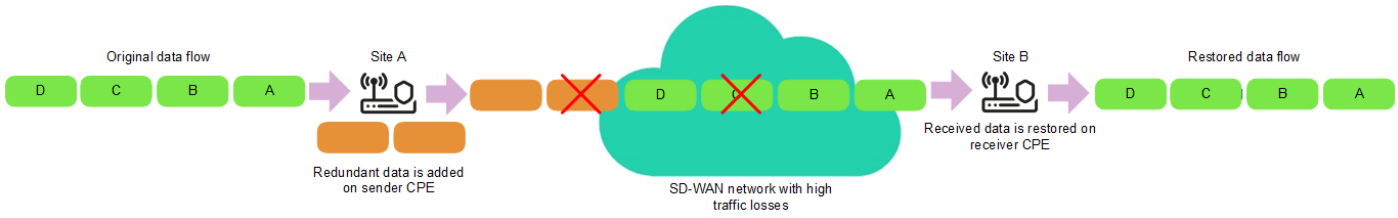


Схема работы функции FEC

Вы можете включить функцию FEC на отдельном туннеле. Туннели отображаются в общей таблице в разделе **Туннели**, в графической топологии в разделе **Топология**, а также в конфигурации устройств CPE на вкладке **Туннели**. В конфигурации устройства CPE отображаются только туннели, построенные с использованием этого устройства.

Для включения функции FEC на туннеле используйте следующие инструкции:

- **Включение функции FEC на туннеле с помощью общей таблицы туннелей**.

  Чтобы включить функцию FEC на туннеле с помощью общей таблицы туннелей:

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

     Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

  2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

     Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

  3. Перейдите в раздел **Туннели**.

     Отобразится таблица туннелей.

  4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **FEC/ реорганизация**.

  5. В открывшемся окне установите флажок **Переопределить**, чтобы настроить FEC на туннеле.

  6. В раскрывающемся списке **Степень избыточности (исходные/дополнительные пакеты)** выберите степень избыточности передаваемых пакетов трафика, которая является соотношением между оригинальными пакетами и дополнительными пакетами, содержащими избыточный код. По умолчанию выбрано значение **0:0 FEC off** и функция не используется.

  7. В поле **Время** введите максимальное время в миллисекундах, в течение которого пакет трафика может находиться в очереди для применения функции FEC. Диапазон значений: от 1 до 1000.

  8. Нажмите на кнопку **Сохранить**.

- Включение функции FEC на туннеле с помощью графической топологии.

  Чтобы включить функцию FEC на туннеле с помощью графической топологии:

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

     Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

  2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

     Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

  3. Перейдите в раздел **Топология**.

     Отобразится топология сети SD-WAN.

  4. Нажмите на туннель и в открывшемся окне нажмите на кнопку **FEC/реорганизация**.

  5. В открывшемся окне установите флажок **Переопределить**, чтобы настроить FEC на туннеле.

  6. В раскрывающемся списке **Степень избыточности (исходные/дополнительные пакеты)** выберите степень избыточности передаваемых пакетов трафика, которая является соотношением между оригинальными пакетами и дополнительными пакетами, содержащими избыточный код. По умолчанию выбрано значение **0:0 FEC off** и функция не используется.

  7. В поле **Время** введите максимальное время в миллисекундах, в течение которого пакет трафика может находиться в очереди для применения функции FEC. Диапазон значений: от 1 до 1000.

  8. Нажмите на кнопку **Сохранить**.

- Включение функции FEC на туннеле в конфигурации устройства CPE.

Чтобы включить функцию FEC на туннеле в конфигурации устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **FEC/реорганизация**.

5. В открывшемся окне установите флажок **Переопределить**, чтобы настроить FEC на туннеле.

6. В раскрывающемся списке **Степень избыточности (исходные/дополнительные пакеты)** выберите степень избыточности передаваемых пакетов трафика, которая является соотношением между оригинальными пакетами и дополнительными пакетами, содержащими избыточный код. По умолчанию выбрано значение **0:0 FEC off** и функция не используется.

7. В поле **Время** введите максимальное время в миллисекундах, в течение которого пакет трафика может находиться в очереди для применения функции FEC. Диапазон значений: от 1 до 1000.

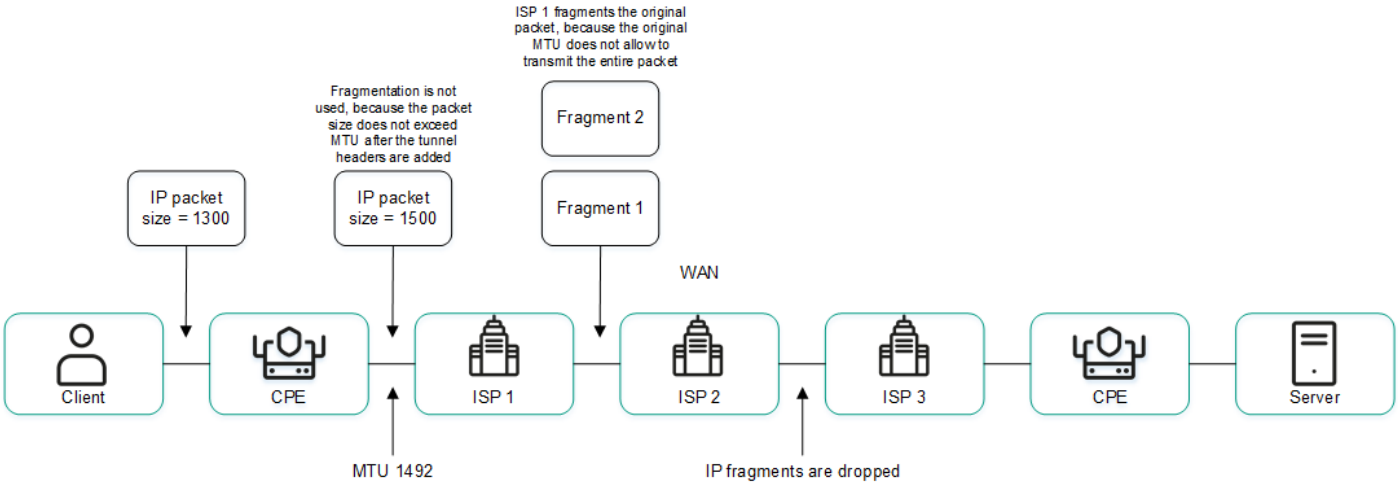
8. Нажмите на кнопку **Сохранить**.

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

Определение эффективного MTU внутри туннеля

Kaspersky SD-WAN может определять поддерживаемый размер MTU (англ. maximum transmission unit) на туннелях между двумя устройствами (устройством CPE и шлюзом SD-WAN или между двумя устройствами CPE).

Определение максимального размера MTU на туннелях необходимо, чтобы обеспечивать прохождение пользовательского трафика через сеть SD-WAN, когда MTU в физической сети (англ. underlay network) занижен и на следующем хопе происходит блокирование фрагментированных пакетов (см. рисунок ниже).



Пример канала связи с пониженным размером MTU и сбросом фрагментированных пакетов

Вычисление поддерживаемого размера MTU осуществляется с помощью отправки пакетов LLDP с переменным размером полезной нагрузки (англ. payload) через все туннели на устройстве CPE и на шлюзе SD-WAN. Минимальный определяемый размер MTU составляет 1280 байт, максимальный – 1500 байт.

Вычисление поддерживаемого размера MTU выполняется:

- При включении устройства CPE.
- С периодичностью, заданной в свойстве `topology.link.pmtud.scheduler.interval.sec` контроллера SD-WAN. По умолчанию задана периодичность 86 400 секунд.
- Вручную по вашему запросу.

Вы можете вычислить поддерживаемый размер MTU на отдельном туннеле. Туннели отображаются в общей таблице в разделе **Туннели**, в графической топологии в разделе **Топология**, а также в конфигурации устройств CPE на вкладке **Туннели**. В конфигурации устройства CPE отображаются только туннели, построенные с использованием этого устройства.

Значения поддерживаемого размера MTU отображаются в столбце **MTU** таблицы туннелей. Если значение еще не подсчитано, отображается значение *Неизвестно*.

Для вычисления MTU на туннеле используйте следующие инструкции:

- **Вычисление MTU на туннеле с помощью общей таблицы туннелей**

Чтобы вычислить MTU на туннеле с помощью общей таблицы туннелей:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Проверить MTU**.

Результат проверки отобразится в столбце **MTU**.

- **Вычисление MTU на туннеле в конфигурации устройства CPE**.

Чтобы вычислить MTU на туннеле в конфигурации устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Проверить MTU**.

Результат проверки отобразится в столбце **MTU**.

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, или в файле настройки контроллера.

Отправленные ICMP-запросы имеют размер пакета 1600 байт. Если хотя бы один из этих запросов получает ответ, проверка фрагментации пакетов на устройстве CPE считается успешной. Вы можете просмотреть результат проверки фрагментации в столбце **Фрагментация** таблицы устройств CPE или таблицы каналов.

Шифрование трафика

Шифрование трафика – это механизм, обеспечивающий безопасную передачу трафика между устройствами CPE через туннели. Например, вы можете использовать шифрование трафика при передаче данных между устройствами по туннелю, построенному поверх незащищенного интернет-соединения.

Контроллер SD-WAN автоматически генерирует ключи для шифрования и дешифровки трафика и передает их на устройства CPE. Трафик шифруется на устройстве-отправителе с помощью ключа для шифрования перед передачей в туннель. Устройство-получатель принимает трафик из туннеля и дешифрует его 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 будут обновляться на устройствах CPE, с помощью свойства `Dtopology.link.encryption.key.update.interval.minutes` контроллера SD-WAN.

> Шифрование трафика поддерживается только на устройствах CPE с программным обеспечением Kaspersky SD-WAN.

Если шифрование трафика включено на устройстве CPE, все исходящие туннели, построенные с использованием этого устройства, передают зашифрованный трафик (включая новые туннели, которые будут построены позже).

Если шифрование трафика выключено на устройстве CPE, оно передает незашифрованный трафик. Обратите внимание, что при выключении шифрования трафика на устройстве, которое до этого передавало зашифрованный трафик, ключи, сгенерированные контроллером SD-WAN для шифрования и дешифровки трафика, удаляются со всех связанных устройств.

Функция шифрования трафика также может быть включена или выключена на туннелях. Например, вы можете включить шифрование трафика на устройстве CPE, но выключить его на туннеле, который построен с использованием этого устройства. При включении или выключении шифрования трафика на туннеле вам нужно одинаковым образом настроить как исходящий, так и входящий туннели.

Шифрование трафика на устройстве CPE

Если на устройстве CPE включено шифрование трафика, по всем туннелям, построенным с его использованием, передается зашифрованный трафик. Исключение составляют случаи, когда вы включаете шифрование трафика на устройстве, но выключаете его на отдельном туннеле.

Вы можете включить или выключить шифрование трафика в шаблоне CPE или на отдельном устройстве. Когда вы включаете или выключаете шифрование трафика в шаблоне CPE, оно автоматически включается или выключается на всех использующих шаблон устройствах. По умолчанию шифрование трафика выключено.

Чтобы включить или выключить шифрование трафика в шаблоне CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на 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.

3. Выберите вкладку **Шифрование туннеля**.

   Отобразится политика шифрования трафика.

4. В раскрывающемся списке **Политика шифрования по умолчанию** выберите **Включено** или **Выключено**.

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

Чтобы включить или выключить шифрование трафика на отдельном устройстве CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Шифрование туннеля**.

   Отобразится политика шифрования трафика.

4. Установите флажок **Переопределить**, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры на выбранной вкладке. По умолчанию флажок снят.

5. В раскрывающемся списке **Политика шифрования по умолчанию** выберите **Включено** или **Выключено**.

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

Шифрование трафика на туннеле

Вы можете включить или выключить шифрование трафика на отдельном туннеле. Туннели отображаются в общей таблице в разделе **Туннели**, в графической топологии в разделе **Топология**, а также в конфигурации устройств CPE на вкладке **Туннели**. В конфигурации устройства CPE отображаются только туннели, построенные с использованием этого устройства.

При включении или выключении шифрования трафика на отдельном туннеле вам нужно одинаковым образом настроить аналогичный встречный туннель. Для включения и выключения шифрования трафика на туннеле используйте следующие инструкции:

- **Включение и выключение шифрования трафика на туннеле с помощью общей таблицы туннелей**.

Чтобы включить или выключить шифрование трафика на туннеле с помощью общей таблицы туннелей:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Включить шифрование**.

5. В открывшемся окне установите или снимите флажок **Переопределить**, чтобы включить или выключить шифрование выбранного туннеля. По умолчанию флажок снят.

6. Установите или снимите флажок **Включить шифрование**. По умолчанию флажок снят.

7. Нажмите на кнопку **Сохранить**.

- Включение и выключение шифрования трафика на туннеле с помощью графической топологии.

Чтобы включить или выключить шифрование трафика на туннеле с помощью графической топологии:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Топология**.

   Отобразится топология сети SD-WAN.

4. Нажмите на туннель и в открывшемся окне нажмите на кнопку **Включить шифрование**.

5. В открывшемся окне установите или снимите флажок **Переопределить**, чтобы включить или выключить шифрование выбранного туннеля. По умолчанию флажок снят.

6. Установите или снимите флажок **Включить шифрование**. По умолчанию флажок снят.

7. Нажмите на кнопку **Сохранить**.

- Включение и выключение шифрования трафика на туннеле в конфигурации устройства CPE.

Чтобы включить или выключить шифрование трафика на туннеле в конфигурации устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Включить шифрование**.

5. В открывшемся окне установите или снимите флажок **Переопределить**, чтобы включить или выключить шифрование выбранного туннеля. По умолчанию флажок снят.

6. Установите или снимите флажок **Включить шифрование**. По умолчанию флажок снят.

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

Настройка топологии

На основании туннелей строится *топология*, которая определяет связность устройств в плоскости передачи данных и отвечает за оптимальность прохождения трафика транспортных сервисов. В Kaspersky SD-WAN устройства можно объединить в одну из следующих топологий:

- *Hub-and-Spoke* – топология по умолчанию, в рамках которой туннели между устройствами CPE устанавливаются через шлюз SD-WAN.
- *Full-Mesh* – топология, в рамках которой туннели между устройствами CPE устанавливаются напрямую.
- *Partial-Mesh* – топология, в рамках которой между некоторыми устройствами CPE туннели устанавливаются напрямую.

Каждому устройству CPE назначается роль – стандартное устройство или шлюз SD-WAN. Стандартные устройства автоматически устанавливают туннели со шлюзами SD-WAN, которые в свою очередь устанавливают туннели со всеми устройствами в сети, включая другие шлюзы. По умолчанию все устройства являются стандартными. Роль шлюза SD-WAN необходима, чтобы построить топологию Hub-and-Spoke.

Стандартным устройствам можно назначать топологические теги и делать их транзитными. Если двум устройствам назначен одинаковый топологический тег, между ними автоматически устанавливается туннель. Другие устройства устанавливают туннели через транзитные устройства. С помощью топологических тегов и транзитных устройств строятся топологии Full-Mesh и Partial-Mesh.

Кроме топологических тегов в решении также используются стандартные теги, которые позволяют классифицировать устройства CPE по различным признакам, таким как модель, версия программного обеспечения или адрес расположения, и выполнять с ними групповые действия, например обновление прошивки. Топологические и стандартные теги никак не связаны друг с другом.

О топологии Hub-and-Spoke

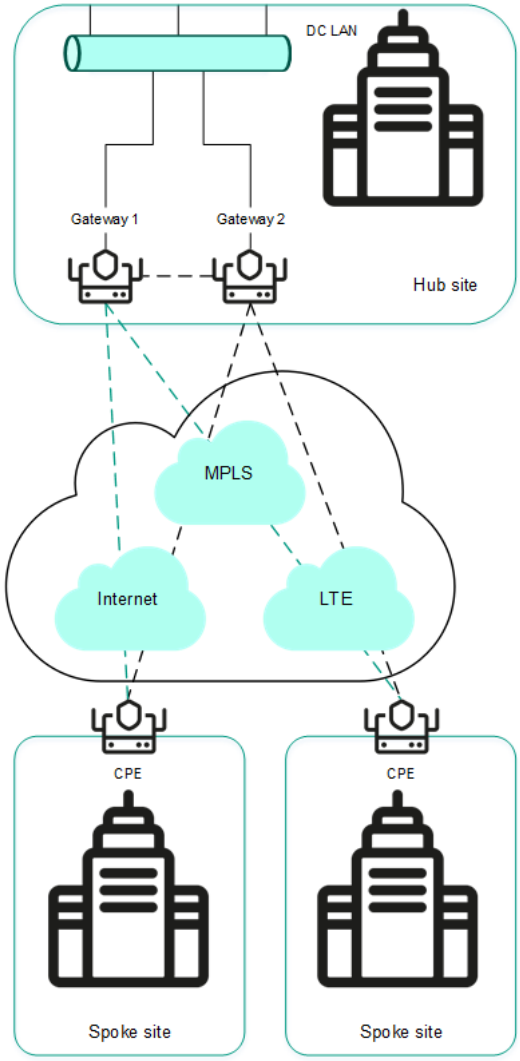
Топология Hub-and-Spoke – это сетевая архитектура, в рамках которой центральная площадка (англ. hub site) подключается к нескольким удаленным площадкам (англ. spoke sites) для обеспечения обмена трафика между ними. Эта топология является наиболее распространенной при построении сетей SD-WAN, так как она 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.

В этой статье описываются примеры таких топологий, которые вы можете построить с помощью Kaspersky SD-WAN. Обратите внимание, что при построении топологии Hub-and-Spoke вы можете использовать качество обслуживания, чтобы ограничить полосу пропускания для устройств CPE или определенных классов трафика.

Hub-and-Spoke без связи между удаленными офисами

На рисунке ниже представлена топология, в рамках которой удаленные площадки подключаются к центральному офису и не могут напрямую связываться 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 центральном ЦОД.

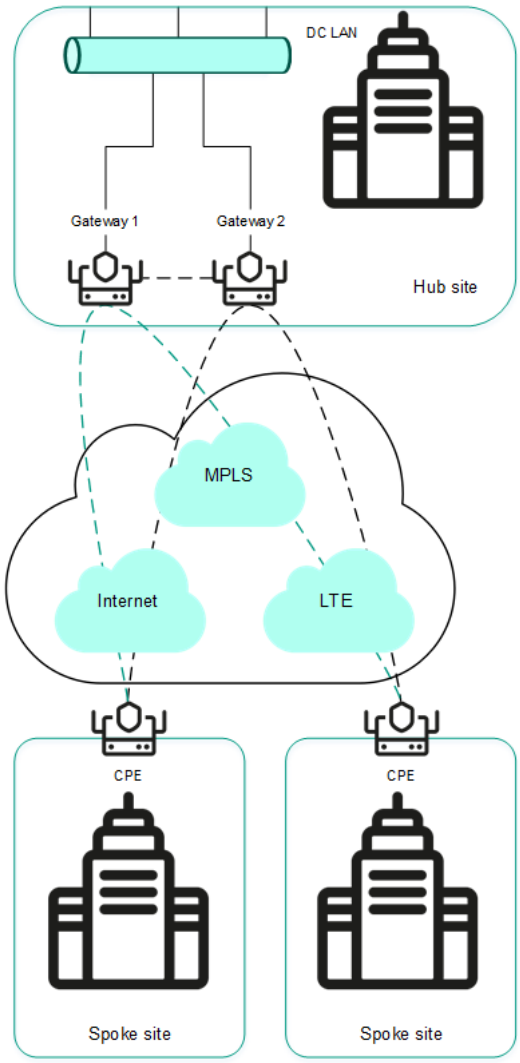
Устройства CPE, регистрирующиеся в оркестраторе, автоматически включаются в управляющий транспортный сервис с ролью Leaf и могут находиться за NAT (Network Address Translation) и PAT (Port Address Translation). В рамках этой топологии невозможна передача трафика напрямую между устройствами.



Топология Hub-and-Spoke без связи между удаленными офисами

Hub-and-Spoke со связью между удаленными офисами через центральный офис

На рисунке ниже представлена топология, в рамках которой удаленные площадки могут связываться друг с другом через центральный офис. Устройства CPE, регистрирующиеся в оркестраторе, автоматически включаются в транспортный сервис и могут находиться за NAT и PAT.



Топология Hub-and-Spoke со связью между удаленными офисами через центральный офис

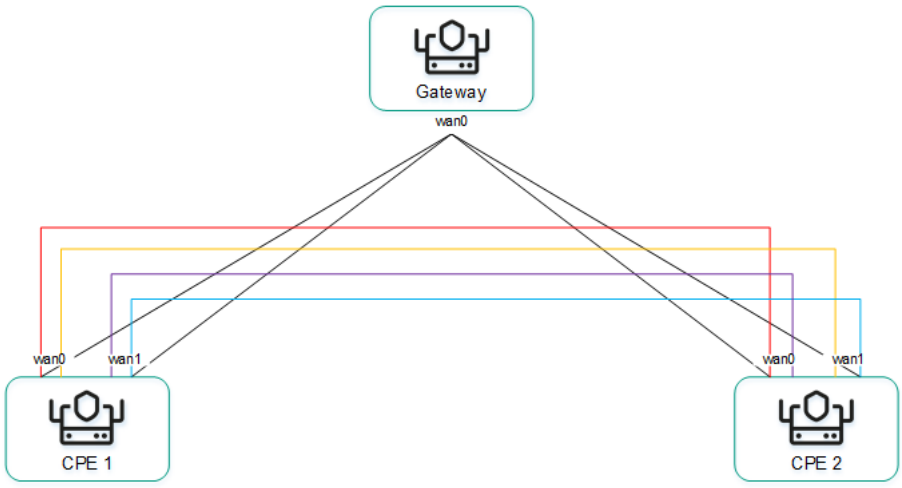
О топологиях Full-Mesh и Partial-Mesh

В Kaspersky SD-WAN поддерживаются топологии Full-Mesh и Partial-Mesh. Для их реализации администратор сети должен предоставить разрешение на динамическое построение прямых туннелей между устройствами CPE.

Построение прямых туннелей между устройствами CPE улучшает производительность Kaspersky SD-WAN благодаря следующим свойствам:

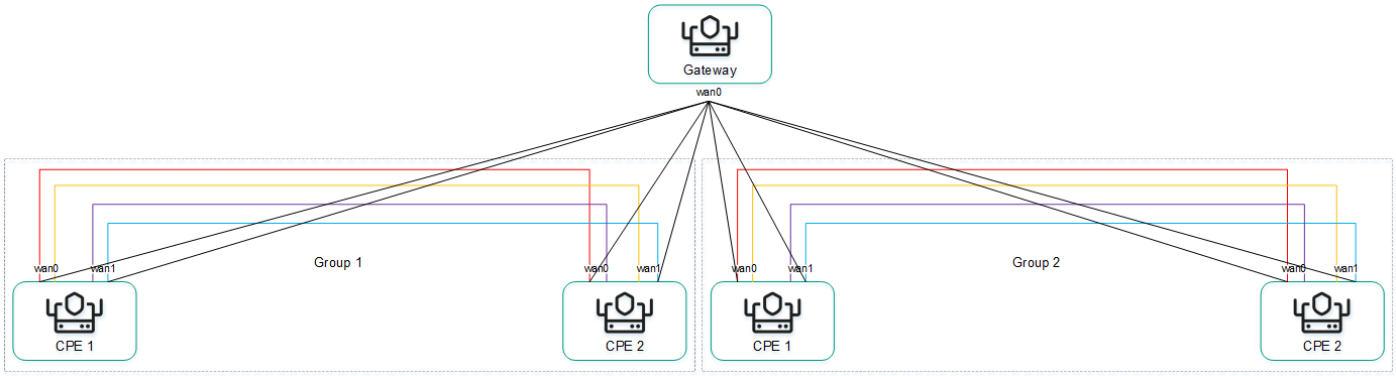
- Улучшенные качественные характеристики физического канала между устройствами CPE, такие как задержка (англ. delay), потеря пакетов (англ. loss) и джиттер (англ. jitter), по сравнению с транзитным сценарием CPE1 → шлюз → CPE2 топологии Hub-and-Spoke.
- Большая пропускная способность прямого физического канала между устройствами CPE, чем в транзитном сценарии CPE1 → шлюз → CPE2.
- Сохранение пропускной способности физического канала передачи данных и аппаратных ресурсов шлюза при использовании прямых связей.

Пример топологии Full-Mesh приведен на рисунке ниже. В этой топологии все устройства CPE строят прямые туннели между собой, используя все имеющиеся физические каналы передачи данных. Таким образом, трафик между устройствами CPE1 и CPE2 пересылается напрямую. Однако при большом количестве устройств CPE и туннелей такая топология может оказаться чрезвычайно требовательной к ресурсам контроллера SD-WAN.



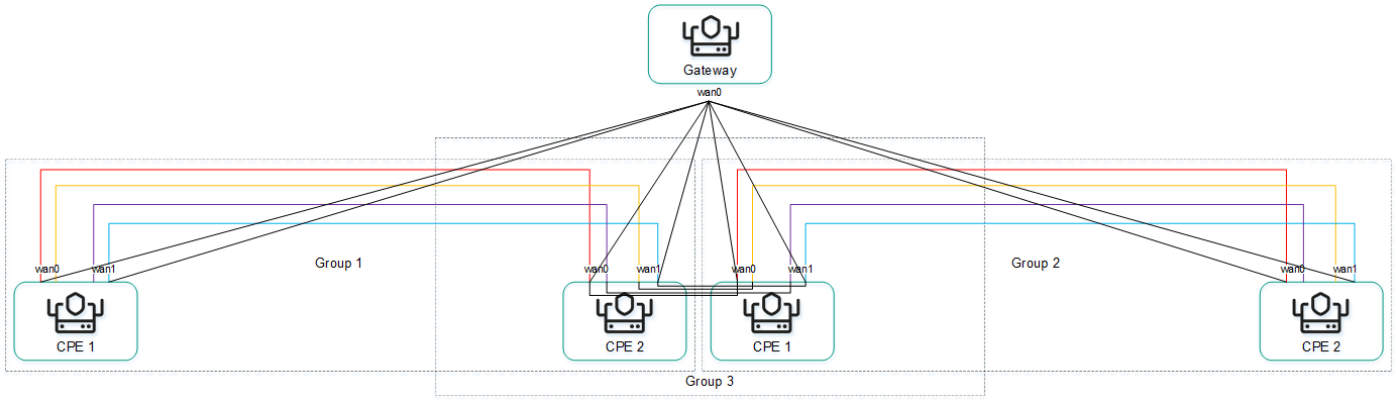
Топология Full-Mesh

Пример топологии Partial-Mesh приведен на рисунке ниже. Такая топология используется в тех случаях, когда прямые туннели между некоторыми устройствами CPE могут быть нежелательны, например, по административным причинам или невозможны по техническим причинам. В этой топологии администратор сети может сгруппировать устройства таким образом, что устройства в одной группе связываются между собой напрямую, а с устройствами из других групп связываются через транзитное устройство.



Топология Partial-Mesh

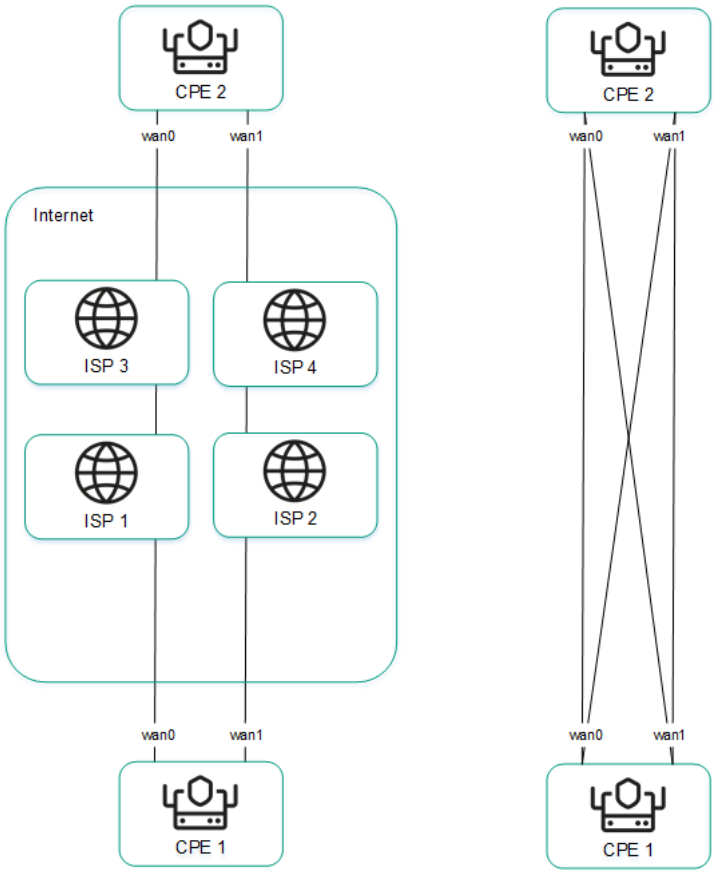
Устройство CPE может входить одновременно в несколько групп, как показано на рисунке ниже.



Топология Partial-Mesh, устройства CPE входят в несколько групп

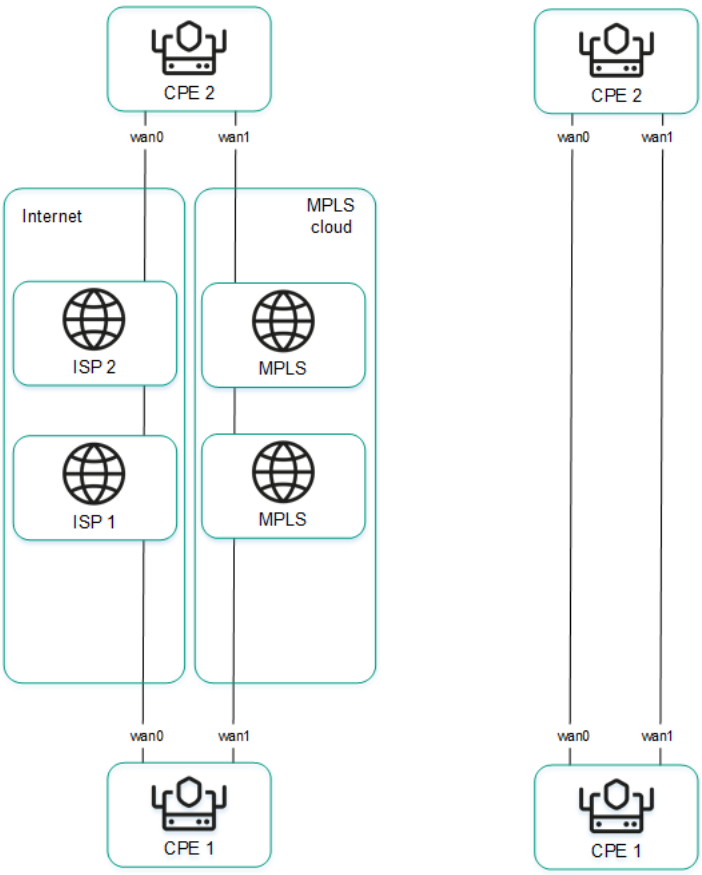
При построении прямых туннелей между устройствами CPE, в зависимости от типа связности устройств через физические каналы, возможны следующие варианты наложенной связности:

- Все физические каналы имеют прямую IP-связность между собой (см. рисунок ниже). За счет связности в пределах интернета устройства CPE могут установить максимальное количество прямых туннелей между собой.



Полная физическая связность между устройствами CPE

- Физические каналы имеют частичную связность (см. рисунок ниже). В примере на рисунке ниже облако интернета и облако MPLS не связаны между собой, поэтому туннели можно установить только через WAN-интерфейсы, принадлежащие одному и тому же облаку. Туннели CPE1:WAN0 → CPE2:WAN1 и CPE1:WAN1 → CPE2:WAN0 установить не получится.



Частичная физическая связность между устройствами CPE

Возможны и другие сценарии связности наложенной сети, если IP-связность между WAN-интерфейсами устройств CPE в пределах одного облака невозможна по другим причинам, например при использовании топологии MPLS, не поддерживающей прямую связь между устройствами, или из-за наличия NAT/PAT или ACL в интернете.

Построение топологии Hub-and-Spoke

Топология Hub-and-Spoke строится с помощью ролей, которые вы назначаете устройствам CPE. Вы можете назначить роль стандартного устройства CPE или шлюза SD-WAN. Стандартные устройства устанавливают туннели друг с другом через шлюзы SD-WAN.

По умолчанию всем устройствам назначена роль стандартного устройства. Для построения топологии Hub-and-Spoke хотя бы одному устройству должна быть назначена роль шлюза SD-WAN.

Вы можете назначить роль в шаблоне CPE или отдельному устройству. Когда вы назначаете роль в шаблоне CPE, эта роль автоматически назначается всем использующим шаблон устройствам. Для построения топологии Hub-and-Spoke используйте следующие инструкции:

- Назначение роли в шаблоне CPE.

Чтобы назначить роль в шаблоне CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на 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.

3. Выберите вкладку **Топология**.

   Отобразятся параметры топологических тегов.

4. В раскрывающемся списке **Роль** выберите роль:

   - **CPE** – стандартное устройство CPE.
   - **Шлюз** – шлюз SD-WAN.

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

- Назначение роли отдельному устройству CPE.

Чтобы назначить роль отдельному устройству CPE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Топологические теги**.

   Отобразятся параметры топологических тегов.

4. В раскрывающемся списке **Коммутатор** выберите устройство CPE.

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

   - **CPE** – стандартное устройство CPE.
   - **Шлюз** – шлюз SD-WAN.

6. Вверху страницы нажмите на кнопку **Сохранить**.

Вы также можете назначить роль в конфигурации устройства CPE.

Чтобы назначить роль в конфигурации устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Топология**.

   Отобразятся параметры топологических тегов.

4. Установите флажок **Переопределить**, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры на выбранной вкладке. По умолчанию флажок снят.

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

   - **CPE** – стандартное устройство CPE.
   - **Шлюз** – шлюз SD-WAN.

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

Построение топологий Full-Mesh и Partial-Mesh

Топологии Full-Mesh и Partial-Mesh строятся с помощью топологических тегов, которые вы назначаете устройствам CPE. Вы можете назначить топологические теги только стандартным устройствам. Если двум устройствам назначен одинаковый топологический тег, между ними автоматически устанавливается туннель.

В топологии Full-Mesh всем устройствам назначается одинаковый топологический тег.

В топологии Partial-Mesh устройства разделяются на группы на основании назначенных им тегов, и связь между ними осуществляют транзитные устройства, которым назначены теги всех групп.

Вы можете назначить топологический тег в шаблоне CPE или отдельному устройству. Когда вы назначаете топологический тег в шаблоне CPE, это тег автоматически назначается всем использующим шаблон устройствам. Для назначения топологических тегов используйте следующие инструкции:

- Назначение топологического тега в шаблоне CPE.

  Чтобы назначить топологический тег в шаблоне CPE:

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

     Отобразится таблица шаблонов CPE.

  2. Нажмите на 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.

  3. Выберите вкладку **Топология**.

     Отобразятся параметры топологических тегов.

  4. Убедитесь, что в раскрывающемся списке **Роль** выбрано значение **CPE**. Роль **Шлюз** не используется для построения топологий Full-Mesh и Partial-Mesh.

  5. Если вы хотите построить топологию Partial-Mesh, при необходимости использовать устройство как транзитное установите флажок **Транзитное устройство CPE**. Транзитные устройство нужны, чтобы связать между собой группы устройств и чтобы другие устройства могли устанавливать туннели через эти устройства.

  6. В поле **Топологические теги** введите топологический тег и нажмите на кнопку добавления +. Устройства с одинаковыми топологическими тегами автоматически устанавливают друг с другом прямые туннели.

     Для построения топологии Full-Mesh назначьте всем устройствам одинаковые топологические теги.

     Для построения топологии Partial-Mesh назначьте устройствам топологические теги в соответствии с тем, к какой группе они относятся. Также назначьте транзитному устройству все используемые в топологии теги, чтобы все группы устройств были добавлены в топологию.

     Топологический тег будет назначен и отобразится под полем **Топологические теги**.

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

- Назначение топологического тега отдельному устройству CPE.

Чтобы назначить топологический тег отдельному устройству CPE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Топологические теги**.

   Отобразятся параметры топологических тегов.

4. В раскрывающемся списке **Коммутатор** выберите устройство CPE.

5. Убедитесь, что в раскрывающемся списке **Роль** выбрано значение **CPE**. Роль **Шлюз** не используется для построения топологий Full-Mesh и Partial-Mesh.

6. Если вы хотите построить топологию Partial-Mesh, при необходимости использовать устройство как транзитное установите флажок **Транзитное устройство CPE**. Транзитные устройство нужны, чтобы связать между собой группы устройств и чтобы другие устройства могли устанавливать туннели через эти устройства.

7. В поле **Топологические теги** введите топологический тег и нажмите на кнопку добавления +. Устройства с одинаковыми топологическими тегами автоматически устанавливают друг с другом прямые туннели.

   Для построения топологии Full-Mesh назначьте всем устройствам одинаковые топологические теги.

   Для построения топологии Partial-Mesh назначьте устройствам топологические теги в соответствии с тем, к какой группе они относятся. Также назначьте транзитному устройству все используемые в топологии теги, чтобы все группы устройств были добавлены в топологию.

   Топологический тег будет назначен и отобразится под полем **Топологические теги**.

8. Вверху страницы нажмите на кнопку **Сохранить**.

Вы также можете назначить топологический тег в конфигурации устройства CPE.

Чтобы назначить топологический тег в конфигурации устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Топология**.

   Отобразятся параметры топологических тегов.

4. Установите флажок **Переопределить**, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры на выбранной вкладке. По умолчанию флажок снят.

5. В раскрывающемся списке **Коммутатор** выберите устройство CPE.

6. Убедитесь, что в раскрывающемся списке **Роль** выбрано значение **CPE**. Роль **Шлюз** не используется для построения топологий Full-Mesh и Partial-Mesh.

7. Если вы хотите построить топологию Partial-Mesh, при необходимости использовать устройство как транзитное установите флажок **Транзитное устройство CPE**. Транзитные устройство нужны, чтобы связать между собой группы устройств и чтобы другие устройства могли устанавливать туннели через эти устройства.

8. В поле **Топологические теги** введите топологический тег и нажмите на кнопку добавления +. Устройства с одинаковыми топологическими тегами автоматически устанавливают друг с другом прямые туннели.

   Для построения топологии Full-Mesh назначьте всем устройствам одинаковые топологические теги.

   Для построения топологии Partial-Mesh назначьте устройствам топологические теги в соответствии с тем, к какой группе они относятся. Также назначьте транзитному устройству все используемые в топологии теги, чтобы все группы устройств были добавлены в топологию.

   Топологический тег будет назначен и отобразится под полем **Топологические теги**.

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

При необходимости вы можете удалить топологический тег в шаблоне CPE или на отдельном устройстве. Для удаления топологических тегов используйте следующие инструкции:

- Удаление топологического тега в шаблоне CPE.

  Чтобы удалить топологический тег в шаблоне CPE:

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

     Отобразится таблица шаблонов CPE.

  2. Нажмите на 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.

  3. Выберите вкладку **Топология**.

     Отобразятся параметры топологических тегов.

  4. Нажмите на кнопку удаления × рядом с топологическим тегом.

     Топологический тег будет удален и перестанет отображаться.

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

- Удаление топологического тега на отдельном устройстве CPE.

Чтобы удалить топологический тег на отдельном устройстве CPE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Топологические теги**.

   Отобразятся параметры топологических тегов.

4. В раскрывающемся списке **Коммутатор** выберите устройство CPE.

5. Нажмите на кнопку удаления ✕ рядом с топологическим тегом.

   Топологический тег будет удален и перестанет отображаться.

6. Вверху страницы нажмите на кнопку **Сохранить**.

Вы также можете удалить топологический тег в конфигурации устройства CPE.

Чтобы удалить топологический тег в конфигурации устройства CPE:

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

   Отобразится таблица устройств CPE.

2. Нажмите на устройство CPE.

   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 текущая конфигурация устройства CPE. На этой вкладке также отображается таблица конфигураций устройства CPE **Внеполосное управление**.

3. Выберите вкладку **Топология**.

   Отобразятся параметры топологических тегов.

4. Установите флажок **Переопределить**, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры на выбранной вкладке. По умолчанию флажок снят.

5. Нажмите на кнопку удаления ✕ рядом с топологическим тегом.

   Топологический тег будет удален и перестанет отображаться.

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

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* – используются для распределения трафика по очередям и указания приоритета его обработки. Например, один из классов может быть использован для трафика реального времени, для которого требуется обеспечить минимальную потерю пакетов.

- *Классификаторы трафика* – определяют, доверять или нет DSCP-значениям (англ. Differentiated Services Code Point values), выставленным в полях заголовков пакетов трафика, а также соотносят эти значения с классификаторами трафика.

- *QoS-правила* – определяют, ограничивается ли скорость трафика, обрабатываемого классификаторами трафика.

- *Ограничения* – используются в транспортных сервисах для соблюдения соглашений об уровне обслуживания (англ. Service Level Agreement, далее также SLA). Вы можете создать два типа ограничений:

  - *Manual TE* – для добавления транспортных путей Manual-TE в транспортные сервисы. При настройке этого типа ограничений вы можете включить использование транспортного пути Auto-SPF, если транспортные пути Manual-TE недоступны.

  - *Пороговые ограничения* – для построения транспортных путей Auto-TE в транспортных сервисах на основании пороговых значений показателей мониторинга.

  Если на туннеле, используемом в транспортном сервисе, достигаются пороговые значения выбранных показателей мониторинга, этот туннель полностью или частично исключается из расчета транспортного пути Auto-TE. Исключенные частично туннели могут учитываться при расчете транспортного пути Auto-TE при отсутствии альтернативных туннелей, соответствующих ограничению.

  Например, вы можете создать ограничение, которое полностью исключает из расчета транспортного пути Auto-TE туннели, на которых достигнуто пороговое значение показателя потерь пакетов. Таким образом, в транспортном сервисе, использующем это ограничение, трафик передается только по туннелям с низким показателем потерь пакетов.

- *Правила классификации трафика* – используются, чтобы определить в общем потоке данных трафик с указанными значениями полей заголовков L2-L4, а также трафик указанных приложений. Для каждого правила классификации трафика вам необходимо указать порядковый номер и выбрать действие по умолчанию, разрешающее или запрещающее дальнейшую маршрутизацию трафика. Правила классификации добавляются в фильтры трафика.

- *Фильтры трафика* – используются, чтобы обеспечить безопасность путем блокирования избыточного или опасного трафика, классифицировать трафик, а также чтобы соблюсти требования SLA для приложений. Каждый фильтр состоит из одного или нескольких правил классификации трафика.

На WAN- и LAN-интерфейсах может использоваться не более 8 очередей трафика. Для каждой очереди требуется указать минимальную и максимальную скорость в процентах от общей скорости, заданной для всего интерфейса. Сумма всех указанных для очередей значений минимальной скорости передачи не должна превышать 100%.

Очереди имеют строгий приоритет, и не зарезервированная полоса пропускания сначала предлагается трафику из очереди с более высоким приоритетом. Каждой очереди гарантируется минимальная полоса пропускания в соответствии с указанной для нее минимальной скорости. Верхнее ограничение максимальной скорости для более приоритетных очередей необходимо, чтобы предоставить доступ к полосе пропускания трафику из менее приоритетных очередей.

Вы можете настроить очереди при создании или изменении WAN-интерфейсов. В связи с тем, что сейчас Kaspersky SD-WAN не поддерживает создание LAN-интерфейсов, очереди можно настроить только для уже существующих LAN-интерфейсов.

Операторы связи (англ. service providers) могут использовать разные QoS-политики для маркировки очередей в своих сетях и выполнения требований SLA для пропуска клиентского трафика. Поэтому при одновременном подключении к каналам разных операторов связи устройства CPE могут гибко перемаркировывать трафик разных очередей для каждого WAN-интерфейса. Для настройки перемаркировки вам необходимо изменить значение типа обслуживания (англ. Type of Service, далее такжеToS) при настройке очередей на интерфейсе SD-WAN.

Вы можете изменить только значения ToS внешних (туннельных) заголовков пакетов трафика, исходящих из WAN-интерфейсов. Изменение недоступно для значений ToS внутренних заголовков пакетов трафика.

Классы трафика

В этом разделе описана настройка классов трафика.

Классы трафика по умолчанию

В Kaspersky SD-WAN существует классы трафика по умолчанию для обработки и фильтрации разных типов трафика (см. таблицу ниже). Вы можете создать новые классы трафика или изменить существующие. При этом классы трафика по умолчанию подходят для большинства схем развертывания решения, и мы не рекомендуем изменять их.

Классы трафика по умолчанию

Имя	Внутренний тег	Очередь	KOver	Исключить при расчете пути
Best effort	0	0	0	Да
Business normal	1	1	1	Нет
Business critical	2	2	1	Нет
Video	3	3	1	Нет
Conference	4	4	1	Нет
Signaling	5	5	1	Нет
Real time	6	6	1	Нет
Network control	7	7	1	Нет

Параметры по умолчанию, значения которых представлены в таблице, описаны в инструкции по созданию и изменению классов трафика.

Создание и изменение классов трафика

Классы трафика по умолчанию, подходят для большинства схем развертывания решения Kaspersky SD-WAN, и мы не рекомендуем изменять их.

Вы можете создать или изменить от 4 до 8 классов трафика в шаблоне экземпляра SD-WAN или изменить классы трафика в уже развернутом экземпляре SD-WAN. Если вы создаете классы трафика в шаблоне экземпляра SD-WAN и используете этот шаблон для развертывания отдельного экземпляра, такие же классы трафика автоматически создаются в развернутом экземпляре.

Для создания и изменения классов трафика используйте следующие инструкции:

- **Создание классов трафика в шаблоне экземпляра SD-WAN**.

В один из создаваемых вами классов трафика необходимо помещать *управляющий трафик*, который используется для управления инфраструктурой SD-WAN и настройки ее компонентов, включая установку и управление туннелями, обмен маршрутной информацией между устройствами, а также мониторинг состояния и производительности сети. Управляющему трафику рекомендуется назначать наиболее высокий приоритет для обеспечения эффективного и надежного функционирования сети.

Чтобы создать классы трафика в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания. По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

2. Выберите вкладку **Классы трафика**.

   Отобразится таблица классов трафика.

3. Нажмите на кнопку **Изменить**.

4. В открывшемся окне нажмите на кнопку **+ Класс трафика**, чтобы добавить класс трафика.

5. В столбце **Имя** укажите имя для класса трафика.

6. В столбце **Очередь** выберите номер очереди, в которую требуется помещать трафик из выбранного класса. Чем выше указанное значение, тем выше приоритет класса трафика. Вы не можете указать одинаковый приоритет для нескольких классов трафика.

7. В столбце **KOver** выберите коэффициент переподписки скорости передачи трафика, который определяет, во сколько раз может быть увеличена определенная для класса скорость, если общая скорость используется не полностью.

8. Если требуется не учитывать доступную классу трафика скорость при расчете маршрута, установите флажок **Исключить при расчете пути**. Когда флажок установлен, вы не можете выбрать для класса трафика коэффициент **KOver**. По умолчанию флажок установлен рядом с последним в таблице классом трафика (**Best effort**).

9. В раскрывающемся списке **Класс трафика по умолчанию** выберите класс, в который требуется помещать весь не попавший в другие классы трафик. По умолчанию выбран последний в таблице класс трафика (**Best effort**).

10. В раскрывающемся списке **Класс управляющего трафика** выберите класс, в который требуется помещать управляющий трафик. По умолчанию выбран первый в таблице класс трафика (**Network control**).

11. В раскрывающемся списке **Максимальная зарезервированная скорость (%)** выберите процент максимальной скорости передачи трафика, который может быть доступен для одного из созданных классов трафика. Диапазон значений: от 10 до 90. По умолчанию выбрано значение **90**.

12. Нажмите на кнопку **Ок**.

13. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

- Изменение классов трафика в шаблоне экземпляра SD-WAN.

Чтобы изменить класс трафика в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

2. Выберите вкладку **Классы трафика**.

   Отобразится таблица классов трафика.

3. Нажмите на кнопку **Изменить**.

4. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию классов трафика в шаблоне экземпляра SD-WAN.

5. Нажмите на кнопку **Ок**.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

- Изменение классов трафика в уже развернутом экземпляре SD-WAN.

Чтобы изменить классы трафика в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **QoS**.

   По умолчанию выбрана вкладка **Классы трафика**, на которой отображается таблица классов трафика.

4. Нажмите на кнопку **Изменить**.

5. В открывшемся окне в столбце **Имя** укажите имя для класса трафика.

6. В столбце **Очередь** выберите номер очереди, в которую требуется помещать трафик из выбранного класса. Чем выше указанное значение, тем выше приоритет класса трафика. Вы не можете указать одинаковый приоритет для нескольких классов трафика.

7. В столбце **KOver** выберите коэффициент переподписки скорости передачи трафика, который определяет, во сколько раз может быть увеличена определенная для класса скорость, если общая скорость используется не полностью.

8. Если требуется не учитывать доступную классу трафика скорость при расчете маршрута, установите флажок **Исключить при расчете пути**. Когда флажок установлен, вы не можете выбрать для класса трафика коэффициент **KOver**. По умолчанию флажок установлен рядом с последним в таблице классом трафика (**Best effort**).

9. В раскрывающемся списке **Максимальная зарезервированная скорость (%)** выберите процент максимальной скорости передачи трафика, который может быть доступен для одного из созданных классов трафика. Диапазон значений: от 10 до 90. По умолчанию выбрано значение **90**.

10. Нажмите на кнопку **Ок**.

Классификаторы трафика

В этом разделе описана настройка классификаторов трафика.

Создание классификатора трафика

Вы можете создать классификатор трафика в шаблоне экземпляра SD-WAN или уже развернутом экземпляре. Если вы создаете классификатор трафика в шаблоне экземпляра SD-WAN и используете этот шаблон для развертывания отдельного экземпляра, такой же классификатор трафика автоматически создается в развернутом экземпляре.

Для создания классификатора трафика используйте следующие инструкции:

- Создание классификатора трафика в шаблоне экземпляра SD-WAN.

  Чтобы создать классификатор трафика в шаблоне экземпляра SD-WAN:

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

     Отобразится таблица шаблонов экземпляров SD-WAN.

     В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания. По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

  2. Выберите вкладку **Классификаторы**.

     Отобразится таблица классификаторов трафика.

  3. Нажмите на кнопку **+ Классификатор**.

  4. В открывшемся окне в поле **Имя** введите имя классификатора трафика.

  5. В списке **Тип** выберите одно из следующих значений:

     - **Trust** – классификатор, доверяющий DSCP-значениям, выставленным в полях заголовков пакетов трафика. Это значение выбрано по умолчанию.
     - **Untrust** – классификатор, не доверяющий DSCP-значениям, выставленным в полях заголовков пакетов трафика.

  6. Если в списке **Тип** вы выбрали **Trust**, установите соответствие между классами и DSCP-значениями в заголовках пакетов трафика:

     a. В столбце **Класс трафика** выберите класс, в который требуется помещать трафик.

     b. В столбце **Внешняя метка** нажмите на кнопку **Выбрать** рядом с заголовком пакета, который должен содержать требуемое DSCP-значение.

     c. Установите флажки рядом с отобразившимися DSCP-значениями, которые должны быть в заголовке пакета для помещения трафика в выбранный класс.

     d. Нажмите на кнопку **Ок**.

  7. Если в списке **Тип** вы выбрали **Untrust**, в раскрывающемся списке **Класс трафика** выберите класс, в который требуется помещать весь трафик.

  8. Нажмите на кнопку **Создать**.

     Классификатор трафика будет создан и отобразится в таблице.

  9. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

- Создание классификатора трафика в уже развернутом экземпляре SD-WAN.

Чтобы создать классификатор трафика в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **QoS**.

   По умолчанию выбрана вкладка **Классы трафика**, на которой отображается таблица классов трафика.

4. Выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

5. Нажмите на кнопку **+ Классификатор**.

6. В открывшемся окне в поле **Имя** введите имя классификатора трафика.

7. В списке **Тип** выберите одно из следующих значений:

   - **Trust** – классификатор, доверяющий DSCP-значениям, выставленным в полях заголовков пакетов трафика. Это значение выбрано по умолчанию.
   - **Untrust** – классификатор, не доверяющий DSCP-значениям, выставленным в полях заголовков пакетов трафика.

8. Если в списке **Тип** вы выбрали **Trust**, установите соответствие между классами и DSCP-значениями в заголовках пакетов трафика:

   a. В столбце **Класс трафика** выберите класс, в который требуется помещать трафик.

   b. В столбце **Внешняя метка** нажмите на кнопку **Выбрать** рядом с заголовком пакета, который должен содержать требуемое DSCP-значение.

   c. Установите флажки рядом с отобразившимися DSCP-значениями, которые должны быть в заголовке пакета для помещения трафика в выбранный класс.

   d. Нажмите на кнопку **Ок**.

9. Если в списке **Тип** вы выбрали **Untrust**, в раскрывающемся списке **Класс трафика** выберите класс, в который требуется помещать весь трафик.

10. Нажмите на кнопку **Создать**.

Классификатор трафика будет создан и отобразится в таблице.

Изменение классификатора трафика

Вы можете изменить классификатор трафика в шаблоне экземпляра SD-WAN или уже развернутом экземпляре. Описание параметров см. в инструкции по созданию классификатора трафика.

Чтобы изменить классификатор трафика в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

2. Выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

3. Нажмите на кнопку **Управление** рядом с классификатором трафика и в раскрывающемся списке выберите **Изменить**.

4. В открывшемся окне измените требуемые параметры.

5. Нажмите на кнопку **Сохранить**.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Чтобы изменить классификатор трафика в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление → Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **QoS**.

   По умолчанию выбрана вкладка **Классы трафика**, на которой отображается таблица классов трафика.

4. Выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

5. Нажмите на кнопку **Управление** рядом с классификатором трафика и в раскрывающемся списке выберите **Изменить**.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

Удаление классификатора трафика

Вы можете удалить классификатор трафика в шаблоне экземпляра SD-WAN или уже развернутом экземпляре. Удаленные классификаторы трафика невозможно восстановить.

Чтобы удалить классификатор трафика в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

2. Выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

3. Нажмите на кнопку **Управление** рядом с классификатором трафика и в раскрывающемся списке выберите **Удалить**.

   Классификатор трафика будет удален и перестанет отображаться в таблице.

4. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Чтобы удалить классификатор трафика в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **QoS**.

   По умолчанию выбрана вкладка **Классы трафика**, на которой отображается таблица классов трафика.

4. Выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

5. Нажмите на кнопку **Управление** рядом с классификатором трафика и в раскрывающемся списке выберите **Удалить**.

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

Классификатор трафика будет удален и перестанет отображаться в таблице.

QoS-правила

В этом разделе описана настройка QoS-правил.

Создание QoS-правила

Вы можете создать QoS-правило в шаблоне экземпляра SD-WAN или уже развернутом экземпляре. Если вы создаете QoS-правило в шаблоне экземпляра SD-WAN и используете этот шаблон для развертывания отдельного экземпляра, такое же QoS-правило автоматически создается в развернутом экземпляре.

Перед созданием QoS-правила требуется создать классификатор трафика.

Для создания QoS-правила используйте следующие инструкции:

- **Создание QoS-правила в шаблоне экземпляра SD-WAN**.

Чтобы создать QoS-правило в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания . По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

2. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

3. Нажмите на кнопку **+ QoS-правило**.

4. В открывшемся окне в поле **Имя** введите имя QoS-правила.

5. В раскрывающемся списке **Классификатор** выберите ранее созданный классификатор трафика, который требуется использовать в QoS-правиле.

6. Настройте ограничение скорости трафика:

   - Если вы хотите не ограничивать скорость трафика, обрабатываемого выбранным ранее классификатором, установите флажок **Не ограничено**.
   - Если вы хотите ограничивать скорость трафика, обрабатываемого выбранным ранее классификатором, снимите флажок **Не ограничено**.

   По умолчанию флажок установлен.

   QoS-правила, не ограничивающие скорость трафика, предоставляют пользователям наиболее производительную сеть, особенно при работе с приложениями и сервисами, которые требуют наличия высокой пропускной способности. Однако если ваша сеть не имеет большого количества ресурсов, ограничение скорости позволяет избежать перегрузок, а также проблем с производительностью и фильтрацией трафика приложений, имеющих разный приоритет.

7. Если вы сняли флажок **Не ограничено**, настройте параметры ограничения скорости трафика:

   a. В поле **MBR** введите максимальную скорость трафика (англ. Maximum Bit Rate). По умолчанию указано значение `1`.

   b. В раскрывающемся списке **Тип скорости** выберите единицы измерения максимальной скорости трафика:

      - **Кбит/сек** – это значение выбрано по умолчанию.
      - **Мбит/сек**.
      - **Гбит/сек**.

   c. Если в раскрывающемся списке **Классификатор** вы выбрали классификатор с типом **Trust**, в раскрывающемся списке **Классификатор**, в столбце **Максимальная зарезервированная скорость (%)** укажите процент от общей скорости трафика, доступный каждому классу. Сумма значений, указанных для каждого класса, должна быть равна 100%.

8. Нажмите на кнопку **Создать**.

   QoS-правило будет создано и отобразится в таблице.

9. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

- Создание QoS-правила в уже развернутом экземпляре SD-WAN.

Чтобы создать QoS-правило в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **QoS**.

   По умолчанию выбрана вкладка **Классы трафика**, на которой отображается таблица классов трафика.

4. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

5. Нажмите на кнопку **+ QoS-правило**.

6. В открывшемся окне в поле **Имя** введите имя QoS-правила.

7. В раскрывающемся списке **Классификатор** выберите ранее созданный классификатор трафика, который требуется использовать в QoS-правиле.

8. Настройте ограничение скорости трафика:

   - Если вы хотите не ограничивать скорость трафика, обрабатываемого выбранным ранее классификатором, установите флажок **Не ограничено**.
   - Если вы хотите ограничивать скорость трафика, обрабатываемого выбранным ранее классификатором, снимите флажок **Не ограничено**.

   По умолчанию флажок установлен.

   QoS-правила, не ограничивающие скорость трафика, предоставляют пользователям наиболее производительную сеть, особенно при работе с приложениями и сервисами, которые требуют наличия высокой пропускной способности. Однако если ваша сеть не имеет большого количества ресурсов, ограничение скорости позволяет избежать перегрузок, а также проблем с производительностью и фильтрацией трафика приложений, имеющих разный приоритет.

9. Если вы сняли флажок **Не ограничено**, настройте параметры ограничения скорости трафика:

   a. В поле **MBR** введите максимальную скорость трафика (англ. Maximum Bit Rate). По умолчанию указано значение `1`.

   b. В раскрывающемся списке **Тип скорости** выберите единицы измерения максимальной скорости трафика:

      - **Кбит/сек** – это значение выбрано по умолчанию.
      - **Мбит/сек**.
      - **Гбит/сек**.

c. Если в раскрывающемся списке **Классификатор** вы выбрали классификатор с типом **Trust**, в раскрывающемся списке **Классификатор**, в столбце **Максимальная зарезервированная скорость (%)** укажите процент от общей скорости трафика, доступный каждому классу. Сумма значений, указанных для каждого класса, должна быть равна 100%.

10. Нажмите на кнопку **Создать**.

    QoS-правило будет создано и отобразится в таблице.

Изменение QoS-правила

Вы можете изменить QoS-правило в шаблоне экземпляра SD-WAN или уже развернутом экземпляре. Описание параметров см. в инструкции по созданию QoS-правила.

Чтобы изменить QoS-правило в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃⌃. По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

2. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

3. Нажмите на кнопку **Управление** рядом с QoS-правилом и в раскрывающемся списке выберите **Изменить**.

4. В открывшемся окне измените требуемые параметры.

5. Нажмите на кнопку **Сохранить**.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Чтобы изменить QoS-правило в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление → Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **QoS**.

   По умолчанию выбрана вкладка **Классы трафика**, на которой отображается таблица классов трафика.

4. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

5. Нажмите на кнопку **Управление** рядом с QoS-правилом и в раскрывающемся списке выберите **Изменить**.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

Удаление QoS-правила

Вы можете удалить QoS-правило в шаблоне экземпляра SD-WAN или уже развернутом экземпляре. Удаленные QoS-правила невозможно восстановить.

Чтобы удалить QoS-правило в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃. По умолчанию будет выбрана вкладка **Информация**, на которой отображается имя шаблона экземпляра SD-WAN.

2. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

3. Нажмите на кнопку **Управление** рядом с QoS-правилом и в раскрывающемся списке выберите **Удалить**.

   QoS-правило будет удалено и перестанет отображаться в таблице.

4. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Чтобы удалить QoS-правило в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление → Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **QoS**.

   По умолчанию выбрана вкладка **Классы трафика**, на которой отображается таблица классов трафика.

4. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

5. Нажмите на кнопку **Управление** рядом с QoS-правилом и в раскрывающемся списке выберите **Удалить**.

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

QoS-правило будет удалено и перестанет отображаться в таблице.

Ограничения

В этом разделе описана настройка ограничений.

Создание ограничения Manual-TE

Перед созданием ограничения Manual-TE требуется создать транспортные пути Manual-TE.

Чтобы создать ограничение Manual-TE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   Отобразится таблица ограничений Manual-TE.

4. Вверху страницы нажмите на кнопку **+ Ограничение Manual-TE**.

5. В открывшемся окне в поле **Имя** введите имя ограничения Manual-TE.

6. Установите флажок **Использовать путь Manual-TE** рядом с транспортными путями Manual-TE, которые требуется добавить в ограничение. По умолчанию флажки сняты и ни один транспортный путь не добавлен в ограничение.

7. При необходимости разрешить использование транспортного пути Auto-SPF в случае недоступности транспортных путей Manual-TE установите флажок **Игнорировать, если путь с ограничением не найден** рядом с требуемыми транспортными путями Manual-TE. Флажок можно установить только рядом с транспортными путями, рядом с которыми установлен флажок **Использовать путь Manual-TE**. По умолчанию флажки сняты и для всех транспортных путей запрещено использование Auto-SPF в качестве альтернативы.

8. Нажмите на кнопку **Создать**.

Ограничение Manual-TE будет создано и отобразится в таблице.

Ограничение Manual-TE можно указать в параметрах транспортного сервиса, чтобы добавить в этот сервис содержащиеся в ограничении транспортные пути Manual-TE.

Изменение ограничения Manual-TE

Чтобы изменить ограничение Manual-TE:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   Отобразится таблица ограничений Manual-TE.

4. Нажмите на кнопку **Управление** рядом с ограничением Manual-TE и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию ограничения Manual-TE.

6. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   Отобразится таблица ограничений Manual-TE.

4. Нажмите на кнопку **Управление** рядом с ограничением Manual-TE и в раскрывающемся списке выберите **Удалить**.

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

Ограничение Manual-TE будет удалено и перестанет отображаться в таблице.

Создание порогового ограничения

Перед созданием порогового ограничения требуется включить мониторинг на туннелях.

Чтобы создать пороговое ограничение:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   Отобразится таблица ограничений Manual-TE.

4. Выберите вкладку **Пороговые ограничения**.

   Отобразится таблица пороговых ограничений.

5. Вверху страницы нажмите на кнопку **+ Пороговое ограничение**.

6. В открывшемся окне в поле **Имя** введите имя порогового ограничения.

7. Установите флажок **Не использовать туннели с пороговым значением** рядом с показателями мониторинга, чтобы ограничение исключало из расчета транспортного пути Auto-TE туннели, на которых достигнуто пороговое значение этих показателей. По умолчанию флажок **Не использовать туннели с пороговым значением** снят и ни один показатель мониторинга не используется для исключения туннелей.

8. При необходимости установите флажок **Игнорировать, если путь с ограничением не найден** рядом с показателями мониторинга, чтобы ограничение не исключало из расчета транспортного пути Auto-TE туннели, на которых достигнуты пороговые значения этих показателей при отсутствии альтернативных туннелей. Флажок можно установить только рядом с туннелями, рядом с которыми установлен флажок **Не использовать туннели с пороговым значением**.

   По умолчанию флажок **Игнорировать, если путь с ограничением не найден** снят и ограничение исключает из расчета транспортного пути Auto-TE все туннели, на которых достигнуты пороговые значения выбранных вами показателей мониторинга.

9. Нажмите на кнопку **Создать**.

Ограничение будет создано отобразится в таблице.

Ограничение можно указать в параметрах транспортного сервиса, чтобы использовать при автоматическом расчете транспортного пути.

Изменение порогового ограничения

Чтобы изменить пороговое ограничение:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   Отобразится таблица ограничений Manual-TE.

4. Выберите вкладку **Пороговые ограничения**.

   Отобразится таблица пороговых ограничений.

5. Нажмите на кнопку **Управление** рядом с пороговым ограничением и в раскрывающемся списке выберите **Изменить**.

6. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию порогового ограничения.

7. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Ограничения**.

   Отобразится таблица ограничений Manual-TE.

4. Выберите вкладку **Пороговые ограничения**.

   Отобразится таблица пороговых ограничений.

5. Нажмите на кнопку **Управление** рядом с пороговым ограничением и в раскрывающемся списке выберите **Удалить**.

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

Пороговое ограничение будет удалено и перестанет отображаться в таблице.

Правила классификации трафика

В этом разделе описана настройка правил классификации трафика.

Создание правила классификации трафика

Чтобы создать правило классификации трафика:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   Отобразится таблица фильтров трафика.

4. Выберите вкладку **Правила**.

   Отобразится таблица правил классификации трафика.

5. Вверху страницы нажмите на кнопку **+ Правило классификации**.

6. В открывшемся окне в поле **Имя** введите имя правила классификации трафика.

7. На вкладке **L2-поля** установите флажки рядом с L2-полями, значения которых правило должно использовать для определения трафика из общего потока данных. Если флажок установлен, введите или выберете требуемое значение. Вы можете использовать значения следующих полей для определения трафика:

   - **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** – доступные значения:
     - **0x0800** – это значение выбрано по умолчанию.
     - **0x86dd**.
     - **0x0806**.

8. Выберите вкладку **L3-поля** и установите флажки рядом с L3-полями, значения которых правило должно использовать для определения трафика из общего потока данных. Если флажок установлен, введите или выберете требуемое значение. Вы можете использовать значения следующих полей для определения трафика:

   - **Протокол** – доступные значения:
     - **IPv4**.
     - **IPv6**.
   - **IP источника** – IPv4-адрес или IPv6-адрес в зависимости от выбранного протокола.
   - **Длина префикса IP источника** – диапазон значений для IPv4-адреса: от 0 до 32; для IPv6-адреса: от 0 до 128.
   - **IP назначения** – IPv4-адрес или IPv6-адрес в зависимости от выбранного протокола.

- **Длина префикса IP назначения** – диапазон значений для IPv4-адреса: от 0 до 32; для IPv6-адреса: от 0 до 128.
- **DSCP**.
- **TOS**.

9. Выберите вкладку **L4-поля** и установите флажки рядом с L4-полями, значения которых правило должно использовать для определения трафика из общего потока данных. Если флажок установлен, введите или выберете требуемое значение. Вы можете использовать значения следующих полей для определения трафика:
   - **IP-протокол**.
   - **Список портов источника**.
   - **Список портов назначения**.
   - **Номер типа ICMP**.
10. Выберите вкладку **DPI** и выберите приложение, трафик которого правило должно определять из общего потока данных:
    a. Установите флажок **Приложение**.
    b. В раскрывающемся списке выберите приложение.

    > Классификация с помощью DPI (Deep Packet Inspection) не поддерживается для трафика, сгенерированного устройствами CPE.

11. Нажмите на кнопку **Создать**.

Правило классификации трафика будет создано и отобразится в таблице.

Правило классификации трафика можно использовать при создании фильтра 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 адрес `192.168.2.0/24`.
  В этом случае правило 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.
  Трафик, у которого отсутствует хотя бы одна из этих характеристик, не определяется.

Изменение правила классификации трафика

Чтобы изменить правило классификации трафика:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   Отобразится таблица фильтров трафика.

4. Выберите вкладку **Правила**.

   Отобразится таблица правил классификации трафика.

5. Нажмите на кнопку **Управление** рядом с правилом классификации трафика и в раскрывающемся списке выберите **Изменить**.

6. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию правила классификации трафика.

7. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   Отобразится таблица фильтров трафика.

4. Выберите вкладку **Правила**.

Отобразится таблица правил классификации трафика.

5. Нажмите на кнопку **Управление** рядом с правилом классификации трафика и в раскрывающемся списке выберите **Удалить**.

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

Правило классификации трафика будет удалено и перестанет отображаться в таблице.

Фильтры трафика

В этом разделе описана настройка фильтров трафика.

Создание фильтра трафика

Перед созданием фильтра трафика требуется создать хотя бы одно правило классификации трафика.

Чтобы создать фильтр трафика:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   Отобразится таблица фильтров трафика.

4. Вверху страницы нажмите на кнопку **+ Фильтр трафика**.

5. В открывшемся окне в поле **Имя** введите имя фильтра трафика.

6. В поле **Порядок** введите порядковый номер правила классификации трафика. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 998. Вы не можете указать одинаковое значение порядкового номера для нескольких правил. По умолчанию указано значение `10`.

7. В раскрывающемся списке **Правило классификации** выберите ранее созданное правило классификации трафика, которое требуется добавить в фильтр.

8. В раскрывающемся списке **Действие** выберите действие, которое правило классификации трафика должно применять к определяемому из общего потока данных трафику:

   - **Разрешить** – разрешить дальнейшую маршрутизацию трафика. Это значение выбрано по умолчанию.
   - **Запретить** – запретить дальнейшую маршрутизацию трафика.

9. Нажмите на кнопку **Добавить**, чтобы добавить ранее созданное правило классификации трафика в фильтр. Вы можете добавить несколько правил.

10. В раскрывающемся списке **Действие по умолчанию (если порядок=999)** выберите действие, которое требуется применять ко всему остальному трафику:

    - **Разрешить** – разрешить дальнейшую маршрутизацию трафика. Это значение выбрано по умолчанию.
    - **Запретить** – запретить дальнейшую маршрутизацию трафика.

11. Нажмите на кнопку **Создать**.

Фильтр трафика будет создан и отобразится в таблице.

Фильтр трафика можно использовать при создании транспортных сервисов.

Изменение фильтра трафика

Чтобы изменить фильтр трафика:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   Отобразится таблица фильтров трафика.

4. Нажмите на кнопку **Управление** рядом с фильтром трафика и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию фильтра трафика.

6. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **Фильтры трафика**.

   Отобразится таблица фильтров трафика.

4. Нажмите на кнопку **Управление** рядом с фильтром трафика и в раскрывающемся списке выберите **Удалить**.

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

Фильтр трафика будет удален и перестанет отображаться в таблице.

Транспортные сервисы

Транспортные сервисы – это механизмы, которые используются для передачи трафика между удаленными площадками и играют критически важную роль в обеспечении надежной, эффективной и безопасной коммуникации через инфраструктуру сети SD-WAN. Транспортные сервисы строятся поверх сегментов и состоят из сервисных интерфейсов.

Kaspersky SD-WAN поддерживает создание следующих транспортных сервисов:

- Point-to-Point (далее также P2P).
- Point-to-Multipoint (далее также P2M).
- Multipoint-to-Multipoint (далее также M2M).
- IP multicast.
- L3 VPN.

При создании транспортных сервисов вы можете добавлять резервные сервисные интерфейсы. Резервные и основные сервисные интерфейсы могут быть созданы на одном устройстве CPE. Использование резервного сервисного интерфейса позволяет продолжать передачу данных в случае выхода из строя основного сервисного интерфейса.

Параметры каждого отдельного транспортного сервиса формируют сервисную топологию, которая определяет тип связности между клиентскими устройствами, подключенными к стандартным устройствам CPE и шлюзам SD-WAN.

Транспортный сервис Point-to-Point (P2P)

Point-to-Point (E-line в классификации MEF, далее также P2P-сервис) –транспортный сервис, в рамках которого устанавливается соединение между двумя сервисными интерфейсами устройств CPE поверх Ethernet-сети для эффективной и безопасной передачи данных без использования промежуточных сетевых устройств. Это особенно актуально при использовании приложений, передающих информацию в реальном времени или обеспечивающих обмен большими файлами.

При создании P2P-сервиса вам нужно указать предающий трафик сервисный интерфейс (далее интерфейс-источник) и принимающий трафик сервисный интерфейс (далее интерфейс-назначение).

Создание P2P-сервиса

Перед созданием P2P-сервиса требуется выполнить следующие действия:

- активировать устройства CPE;
- создать ограничение (Manual-TE или пороговое);
- создать сервисные интерфейсы;
- создать фильтр трафика;

- создать QoS-правило.

Чтобы создать транспортный сервис P2P:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2P-сервисы**.

   Отобразится таблица P2P-сервисов.

4. Вверху страницы нажмите на кнопку **+ P2P-сервис**.

5. В открывшемся окне в поле **Имя** введите имя транспортного сервиса.

6. В раскрывающемся списке **Ограничение** выберите ранее созданное ограничение, которое требуется добавить в транспортный сервис.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для равномерного распределения трафика по туннелям, что позволяет предотвращать перегрузку отдельных туннелей и избегать проблем с производительностью у пользователей:

   - **По потокам** – балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям. Это значение выбрано по умолчанию.
   - **По пакетам** – балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
   - **Широковещательный** – пакеты передаются одновременно во все туннели для исключения потерь.

8. При необходимости в поле **Описание** введите краткое описание P2P-сервиса.

9. В раскрывающихся списках **Коммутатор** и **Порт** слева выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как интерфейс-источник.

10. В раскрывающихся списках **Коммутатор** и **Порт** справа выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как интерфейс-назначение.

11. При необходимости отобразить в раскрывающихся списках **Порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

12. При необходимости поменять местами значения, выбранные в раскрывающемся списке **Порт** для интерфейса-источника и интерфейса-назначения, установите флажок **Переключить интерфейсы**. По умолчанию флажок снят.

13. При необходимости добавьте резервный интерфейс-источник, через который трафик будет передаваться в случае выхода из строя основного интерфейса:

    a. Установите флажок **Резервный интерфейс**. По умолчанию флажок снят.

b. В раскрывающихся списках **Резервный коммутатор** и **Резервный порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как резервный.

c. При необходимости отобразить в раскрывающемся списке **Резервный порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.

14. В раскрывающихся списках **Входящий фильтр** слева и справа выберите ранее созданный фильтр трафика для интерфейса-источника и интерфейса-назначения.

15. В раскрывающемся списке **QoS** выберите ранее созданное QoS-правило для интерфейса-источника.

16. При необходимости отслеживать состояние обоих сервисных интерфейсов и если один из них выключается, автоматически выключить второй установите флажок **Транслировать статус интерфейса**. По умолчанию флажок снят. 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 если на сервисных интерфейсах используется тип инкапсуляции Access. Тип инкапсуляции выбирается при создании сервисного интерфейса.

17. Нажмите на кнопку **Создать**.

P2P-сервис будет создан и отобразится в таблице.

Изменение P2P-сервиса

Чтобы изменить P2P-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2P-сервисом и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию P2P-сервиса.

6. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2P-сервисом и в раскрывающемся списке выберите **Удалить**.

5. При необходимости удалить добавленные в P2P-сервис сервисные интерфейсы в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

6. Нажмите на кнопку **Удалить**.

P2P-сервис будет удален и перестанет отображаться в таблице.

Просмотр статистики работы P2P-сервиса

Чтобы просмотреть статистику работы P2P-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2P-сервисом и в раскрывающемся списке выберите **Статистика**.

Откроется окно со статистикой работы P2P-сервиса.

Настройка отображения устройств в топологии P2P-сервиса

Чтобы настроить отображение устройств в топологии P2P-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2P-сервисы**.

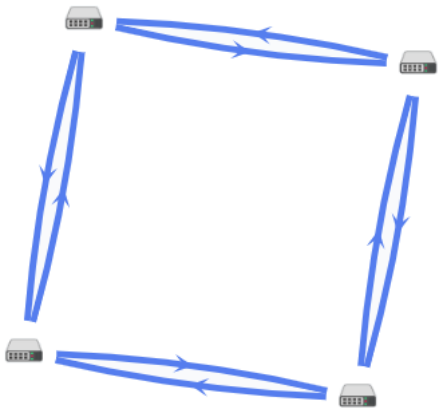
   Отобразится таблица P2P-сервисов.

4. Нажмите на кнопку **Управление** рядом с P2P-сервисом и в раскрывающемся списке выберите **Топология**.

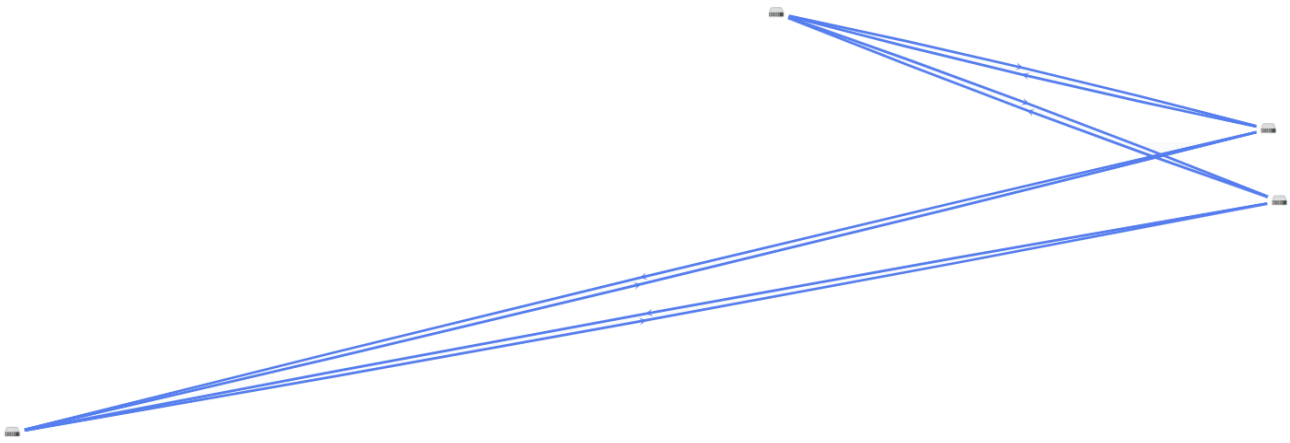
   Откроется окно с топологией P2P-сервиса.

5. При необходимости изменить взаимное расположение устройств CPE в топологии используйте следующие кнопки вверху окна:

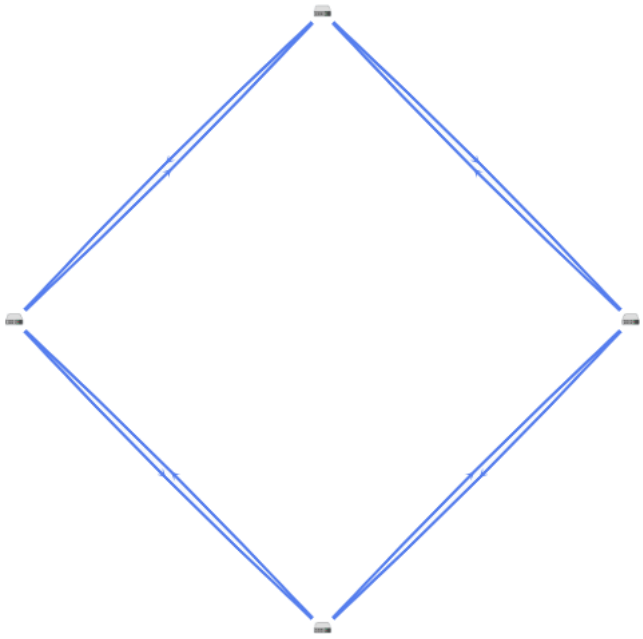
   - **Вручную** – вручную изменить взаимное расположение устройств CPE.
   - **Автоматически** – выбрать одно из значений в раскрывающемся списке, чтобы топология транспортного сервиса была сгенерирована автоматически:
     - **Физическая симуляция** – устройства CPE на схеме располагаются примерно в соответствии с их реальным расположением относительно друг-друга. Например:

     - **Случайно** – устройства CPE располагаются случайным образом. Например:

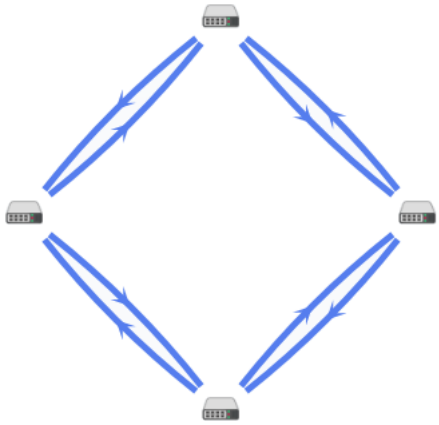
       

     - **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо. Например:



- **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. При необходимости отобразить подписи к устройствам CPE, установите следующие флажки:

   - **Имя**.
   - **IP-адрес**.

   По умолчанию флажки сняты.

7. При необходимости отобразите туннели, используемые в сегменте из двух устройств CPE:

   a. Установите флажок **Сегменты**. По умолчанию флажок снят.

   b. Выберите устройства в раскрывающихся списках снизу или на схеме.

8. При необходимости отобразить окно с кнопками управления и дополнительной информацией об устройстве CPE или туннеле, нажмите на значок устройства или туннеля.

Перезагрузка P2P-сервиса

Перезагрузка P2P-сервиса может потребоваться в случае, если при его функционировании возникла проблема (например с сетевым подключением) или в текущую конфигурацию были внесены требующие перезагрузки изменения.

Чтобы перезагрузить P2P-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2P-сервисом и в раскрывающемся списке выберите **Перезагрузить**.

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

Откроется окно с сообщением об успешной перезагрузке P2P-сервиса. Контроллер SD-WAN добавит P2P-сервис на все устройства CPE, которые ранее использовались в этом сервисе.

Транспортный сервис Point-to-Multipoint (P2M)

Point-to-Multipoint (E-tree в классификации MEF, далее также P2M-сервис) – транспортный сервис, в рамках которого один сервисный интерфейс устройства CPE централизованно передает трафик на несколько интерфейсов поверх Ethernet-сети по принципу топологии *дерево*.

Иерархическая структура P2M-сервиса упрощает процесс управления сетью, обеспечивает надежность передачи данных без дупликации, а также увеличивает масштабируемость сети за счет возможности добавлять новые устройства.

При создании P2M-сервиса вам нужно назначить каждому сервисному интерфейсу одну из следующих ролей:

- **Root** – сервисный интерфейс, который может отправлять трафик на интерфейсы с любой ролью. Эту роль необходимо назначить как минимум одному сервисному интерфейсу.
- **Leaf** – сервисный интерфейс, который может отправлять трафик только на интерфейсы с ролью Root.

Поддерживается передача кадров, соответствующих стандартам IEEE 802.1Q и 802.1AD.

Создание P2M-сервиса

Перед созданием P2M-сервиса требуется выполнить следующие действия:

- активировать устройства CPE;
- создать ограничение (Manual-TE или пороговое);
- создать сервисные интерфейсы;
- определить топологию транспортного сервиса с назначением ролей сервисным интерфейсам;
- создать фильтр трафика;
- создать группу OpenFlow-интерфейсов;
- создать QoS-правило.

Чтобы создать транспортный сервис P2M:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

   Отобразится таблица P2M-сервисов.

4. Вверху страницы нажмите на кнопку **+ P2M-сервис**.

5. В открывшемся окне в поле **Имя** введите имя транспортного сервиса.

6. В раскрывающемся списке **Ограничение** выберите ранее созданное ограничение, которое требуется добавить в транспортный сервис.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для равномерного распределения трафика по туннелям, что позволяет предотвращать перегрузку отдельных туннелей и избегать проблем с производительностью у пользователей:

   - **По потокам** – балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям. Это значение выбрано по умолчанию.
   - **По пакетам** – балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
   - **Широковещательный** – пакеты передаются одновременно во все туннели для исключения потерь.

8. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое вы хотите применять 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 таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отправляется на все добавленные в транспортный сервис сервисные интерфейсы, за исключением интерфейса, на который серия кадров пришла изначально. Значение по умолчанию.

- **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отбрасывается.

> При наличии MAC-адреса назначения в таблице MAC-адресов серия кадров отправляется на сервисный интерфейс назначения.

9. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого вы хотите хранить записи в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. По умолчанию указано значение `300`.

10. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

    - **Flood** – трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Значение по умолчанию.

    - **Drop** – трафик с ранее неизученными MAC-адресами назначения не передается.

11. 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. По умолчанию указано значение `100`.

12. В раскрывающемся списке **Режим** выберите, хотите ли вы использовать Default Forwarding Interface (далее DFI), на который отправляется неизвестный unicast-трафик, в транспортном сервисе:

    - **Классический** – не использовать DFI. Значение по умолчанию.

    - **DFI с FIB на root и leafs** – использовать DFI на сервисном интерфейсе с ролью root. Количество сервисных интерфейсов с ролью leaf не ограничено. Для всех сервисных интерфейсов можно добавить резервные сервисные интерфейсы.

    - **DFI с FIB на leaf** – использовать DFI на сервисном интерфейсе с ролью root. Количество сервисных интерфейсов с ролью leaf не ограничено. Сервисные интерфейсы с ролью leaf должны находиться на одном устройстве CPE. Для всех сервисных интерфейсов можно добавить резервные сервисные интерфейсы.

      Резервные сервисные интерфейсы с ролью leaf должны находиться на одном устройстве CPE, отличном от устройства, на котором находятся основные сервисные интерфейсы.

13. При необходимости в поле **Описание** введите краткое описание транспортного сервиса.

14. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

15. В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется добавить в транспортный сервис.

16. При необходимости отобразить в раскрывающемся списке **Порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

17. В раскрывающемся списке **QoS** выберите ранее созданное QoS-правило для сервисного интерфейса.

18. В раскрывающемся списке **Входящий фильтр** выберите ранее созданный фильтр трафика для сервисного интерфейса.

19. В раскрывающемся списке **Роль** выберите роль сервисного интерфейса:

    - **Leaf**.
    - **Root**.

20. При необходимости добавьте резервный сервисный интерфейс, через который трафик будет передаваться в случае выхода из строя основного интерфейса:

    a. Установите флажок **Резервный интерфейс**. По умолчанию флажок снят.

    b. В раскрывающихся списках **Резервный коммутатор** и **Резервный порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как резервный.

    c. При необходимости отобразить в раскрывающемся списке **Резервный порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

    > Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.

21. При необходимости назначить роль DFI сервисному интерфейсу, установите флажок **Default Forwarding Interface**. Флажок невозможно установить, если в раскрывающемся списке **Роль** вы выбрали **Leaf** для сервисного интерфейса.

22. Нажмите на кнопку **+ Добавить**, чтобы добавить сервисный интерфейс в транспортный сервис.

    Сервисный интерфейс отобразится внизу окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.

23. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

24. В раскрывающемся списке **Группа** выберите ранее созданную группу OpenFlow-интерфейсов, которую требуется добавить. Поверх каждого OpenFlow-интерфейса в группе автоматически создается сервисный интерфейс, который в свою очередь добавляется в транспортный сервис.

25. В раскрывающемся списке **QoS** выберите ранее созданное QoS-правило для сервисных интерфейсов, созданных поверх OpenFlow-интерфейсов.

26. В поле **VLAN ID** введите значение внешней метки VLAN для сервисных интерфейсов, созданных поверх OpenFlow-интерфейсов. Вам нужно учитывать следующие ограничения, касающиеся автоматического создания сервисных интерфейсов поверх OpenFlow-интерфейсов:

    - поддерживается создание только сервисных интерфейсов с типом инкапсуляции VLAN;
    - значение VLAN-метки на всех сервисных интерфейсах должно быть одинаковым.

27. В раскрывающемся списке **Роль** выберите роль для сервисных интерфейсов, автоматически созданных поверх OpenFlow-интерфейсов:

    - **Leaf**.
    - **Root**.

28. Нажмите на кнопку **+ Добавить**, чтобы добавить группу OpenFlow-интерфейсов в транспортный сервис.

    Автоматически созданные сервисные интерфейсы отобразятся внизу окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.

29. Нажмите на кнопку **Создать**.

P2M-сервис будет создан и отобразится в таблице.

Изменение P2M-сервиса

Чтобы изменить P2M-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2M-сервисом и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию P2M-сервиса.

6. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2M-сервисом и в раскрывающемся списке выберите **Удалить**.

5. При необходимости удалить добавленные в P2M-сервис сервисные интерфейсы в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

6. Нажмите на кнопку **Удалить**.

P2M-сервис будет удален и перестанет отображаться в таблице.

Просмотр статистики работы P2M-сервиса

Чтобы просмотреть статистику работы P2M-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2M-сервисом и в раскрывающемся списке выберите **Статистика**.

Откроется окно со статистикой работы P2M-сервиса.

Просмотр MAC-таблицы P2M-сервиса

Чтобы просмотреть MAC-таблицу P2M-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2M-сервисом и в раскрывающемся списке выберите **MAC-таблица**.

   Откроется окно с MAC-таблицей P2M-сервиса.

5. При необходимости найти определенный MAC-адрес введите его в поле и нажмите на кнопку **Найти по MAC**.

6. При необходимости очистить таблицу MAC-адресов нажмите на кнопку **Очистить**.

Настройка отображения устройств в топологии P2M-сервиса

Чтобы настроить отображение устройств в топологии P2M-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **P2M-сервисы**.

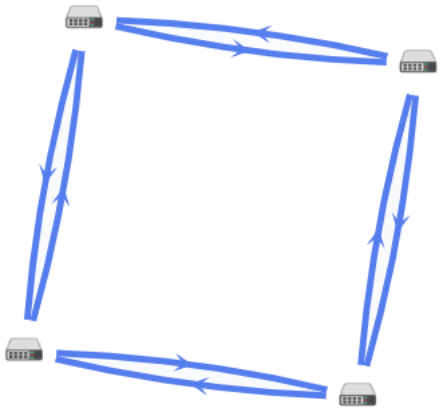
   Отобразится таблица P2M-сервисов.

4. Нажмите на кнопку **Управление** рядом с P2M-сервисом и в раскрывающемся списке выберите **Топология**.

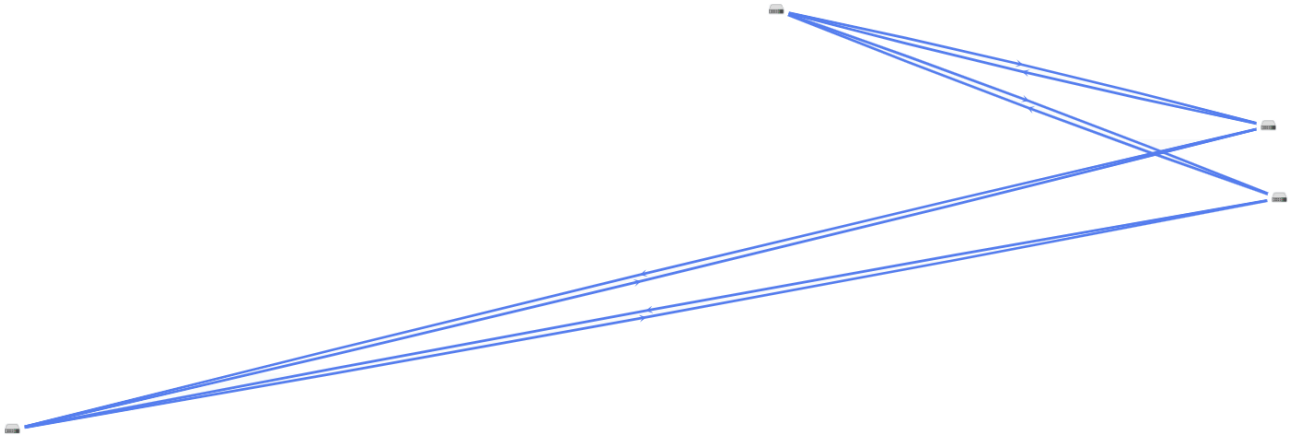
   Откроется окно с топологией P2M-сервиса.

5. При необходимости изменить взаимное расположение устройств CPE в топологии используйте следующие кнопки вверху окна:

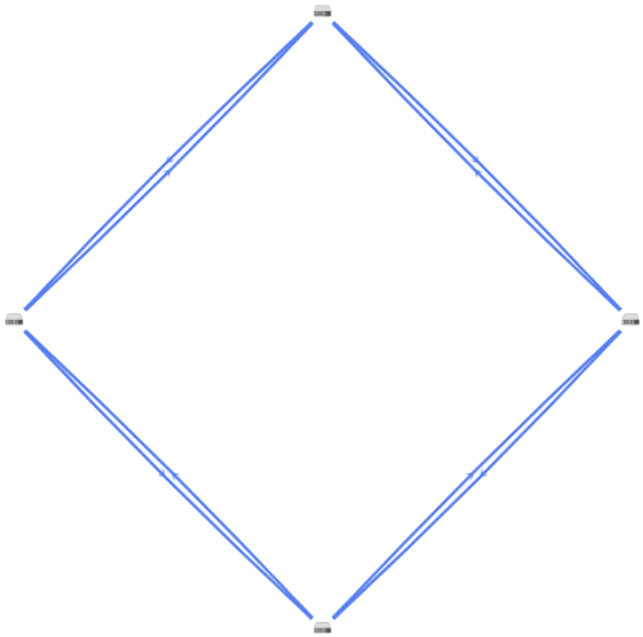
   - **Вручную** – вручную изменить взаимное расположение устройств CPE.
   - **Автоматически** – выбрать одно из значений в раскрывающемся списке, чтобы топология транспортного сервиса была сгенерирована автоматически:
     - **Физическая симуляция** – устройства CPE на схеме располагаются примерно в соответствии с их реальным расположением относительно друг-друга. Например:

     - **Случайно** – устройства CPE располагаются случайным образом. Например:

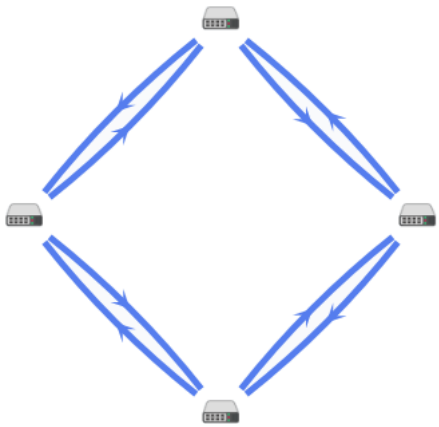


- **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо. Например:



- **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. При необходимости отобразить подписи к устройствам CPE, установите следующие флажки:

- **Имя**.

- **IP-адрес**.

По умолчанию флажки сняты.

7. При необходимости отобразите туннели, используемые в сегменте из двух устройств CPE:

   a. Установите флажок **Сегменты**. По умолчанию флажок снят.

   b. Выберите устройства в раскрывающихся списках снизу или на схеме.

8. При необходимости отобразить окно с кнопками управления и дополнительной информацией об устройстве CPE или туннеле, нажмите на значок устройства или туннеля.

Перезагрузка P2M-сервиса

Перезагрузка P2M-сервиса может потребоваться в случае, если при его функционировании возникла проблема (например с сетевым подключением) или в текущую конфигурацию были внесены требующие перезагрузки изменения.

Чтобы перезагрузить P2M-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с P2M-сервисом и в раскрывающемся списке выберите **Перезагрузить**.

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

Откроется окно с сообщением об успешной перезагрузке P2M-сервиса. Контроллер SD-WAN добавит P2M-сервис на все устройства CPE, которые ранее использовались в этом сервисе.

Транспортный сервис Multipoint-to-Multipoint (M2M)

Multipoint-to-Multipoint (E-LAN в классификации MEF, далее также M2M-сервис) – транспортный сервис, в рамках которого между интерфейсами устройств CPE устанавливается равнозначное соединение поверх локальной Ethernet-сети для обмена данными и совместного выполнения требуемых задач в общей сетевой среде без централизованного контроллера и четкой иерархии.

Для заполнения MAC-таблицы на контроллере SD-WAN M2M-сервис использует механизм изучения MAC-адресов (англ. MAC learning). При этом на каждом устройстве CPE также организуется отдельный bridge-домен и содержится отдельная таблица MAC-адресов.

Создание M2M-сервиса

Перед созданием M2M-сервиса требуется выполнить следующие действия:

- активировать устройства CPE;
- создать ограничение (Manual-TE или пороговое);
- создать сервисные интерфейсы;
- создать фильтр трафика;
- создать группу OpenFlow-интерфейсов;
- создать QoS-правило.

Чтобы создать транспортный сервис M2M:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

   Отобразится таблица M2M-сервисов.

4. Вверху страницы нажмите на кнопку **+ M2M-сервис**.

5. В открывшемся окне в поле **Имя** введите имя транспортного сервиса.

6. В раскрывающемся списке **Ограничение** выберите ранее созданное ограничение, которое требуется добавить в транспортный сервис.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для равномерного распределения трафика по туннелям, что позволяет предотвращать перегрузку отдельных туннелей и избегать проблем с производительностью у пользователей:

   - **По потокам** – балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям. Это значение выбрано по умолчанию.
   - **По пакетам** – балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
   - **Широковещательный** – пакеты передаются одновременно во все туннели для исключения потерь.

8. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое вы хотите применять 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 таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров

отправляется на все добавленные в транспортный сервис сервисные интерфейсы, за исключением интерфейса, на который серия кадров пришла изначально. Значение по умолчанию.

- **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отбрасывается.

  При наличии MAC-адреса назначения в таблице MAC-адресов серия кадров отправляется на сервисный интерфейс назначения.

9. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого вы хотите хранить записи в MAC-таблице контроллера. Диапазон значений: от 10 до 65 535. По умолчанию указано значение `300`.

10. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы контроллера:

    - **Flood** – трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Значение по умолчанию.

    - **Drop** – трафик с ранее неизученными MAC-адресами назначения не передается.

11. 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. По умолчанию указано значение `100`.

12. При необходимости в поле **Описание** введите краткое описание транспортного сервиса.

13. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

14. В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется добавить в транспортный сервис.

15. При необходимости отобразить в раскрывающемся списке **Порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

16. В раскрывающемся списке **QoS** выберите ранее созданное QoS-правило для сервисного интерфейса.

17. В раскрывающемся списке **Входящий фильтр** выберите ранее созданный фильтр трафика для сервисного интерфейса.

18. При необходимости добавьте резервный сервисный интерфейс, через который трафик будет передаваться в случае выхода из строя основного интерфейса:

    a. Установите флажок **Резервный интерфейс**. По умолчанию флажок снят.

    b. В раскрывающихся списках **Резервный коммутатор** и **Резервный порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как резервный.

    c. При необходимости отобразить в раскрывающемся списке **Резервный порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.

19. Нажмите на кнопку **+ Добавить**, чтобы добавить сервисный интерфейс в транспортный сервис.

    Сервисный интерфейс отобразится внизу окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.

20. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

21. В раскрывающемся списке **Группа** выберите ранее созданную группу OpenFlow-интерфейсов, которую требуется добавить. Поверх каждого OpenFlow-интерфейса в группе автоматически создается сервисный интерфейс, который в свою очередь добавляется в транспортный сервис.

22. В раскрывающемся списке **QoS** выберите ранее созданное QoS-правило для сервисных интерфейсов, созданных поверх OpenFlow-интерфейсов.

23. В поле **VLAN ID** введите значение внешней метки VLAN для сервисных интерфейсов, созданных поверх OpenFlow-интерфейсов. Вам нужно учитывать следующие ограничения, касающиеся автоматического создания сервисных интерфейсов поверх OpenFlow-интерфейсов:

    - поддерживается создание только сервисных интерфейсов с типом инкапсуляции VLAN;
    - значение VLAN-метки на всех сервисных интерфейсах должно быть одинаковым.

24. Нажмите на кнопку **+ Добавить**, чтобы добавить группу OpenFlow-интерфейсов в транспортный сервис.

    Автоматически созданные сервисные интерфейсы отобразятся внизу окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.

25. Нажмите на кнопку **Создать**.

M2M-сервис будет создан и отобразится в таблице.

Изменение M2M-сервиса

Чтобы изменить M2M-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с M2M-сервисом и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию M2M-сервиса.

6. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с M2M-сервисом и в раскрывающемся списке выберите **Удалить**.

5. При необходимости удалить добавленные в M2M-сервис сервисные интерфейсы в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

6. Нажмите на кнопку **Удалить**.

M2M-сервис будет удален перестанет отображаться в таблице.

Просмотр статистики работы M2M-сервиса

Чтобы просмотреть статистику работы M2M-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с M2M-сервисом и в раскрывающемся списке выберите **Статистика**.

Откроется окно со статистикой работы M2M-сервиса.

Просмотр MAC-таблицы M2M-сервиса

Чтобы просмотреть MAC-таблицу M2M-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с M2M-сервисом и в раскрывающемся списке выберите **MAC-таблица**.

   Откроется окно с MAC-таблицей M2M-сервиса.

5. При необходимости найти определенный MAC-адрес введите его в поле и нажмите на кнопку **Найти по MAC**.

6. При необходимости очистить таблицу MAC-адресов нажмите на кнопку **Очистить**.

Настройка отображения устройств в топологии M2M-сервиса

Чтобы настроить отображение устройств в топологии M2M-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **M2M-сервисы**.

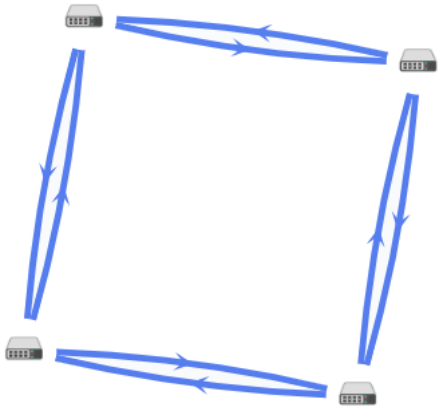
   Отобразится таблица M2M-сервисов.

4. Нажмите на кнопку **Управление** рядом с M2M-сервисом и в раскрывающемся списке выберите **Топология**.

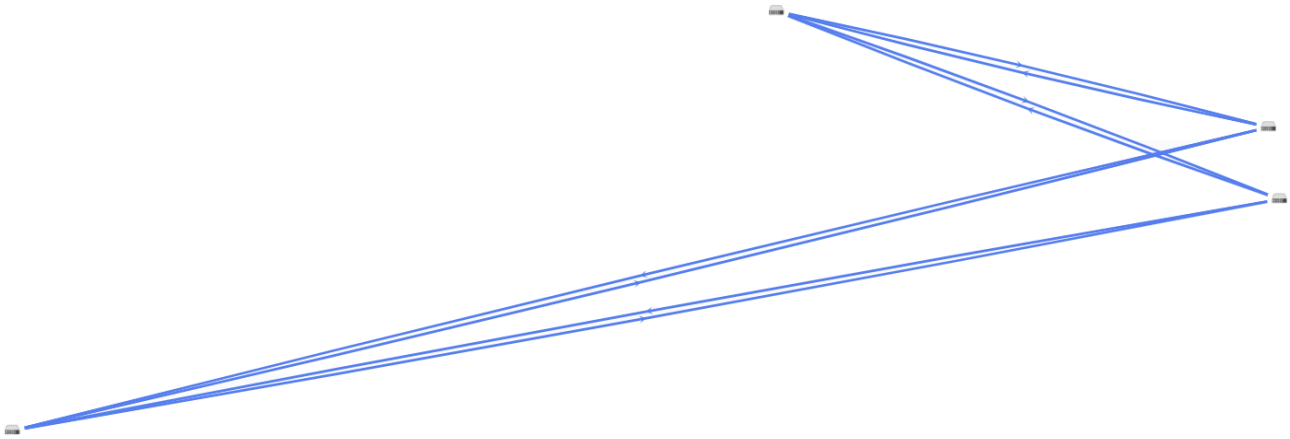
   Откроется окно с топологией M2M-сервиса.

5. При необходимости изменить взаимное расположение устройств CPE в топологии используйте следующие кнопки вверху окна:

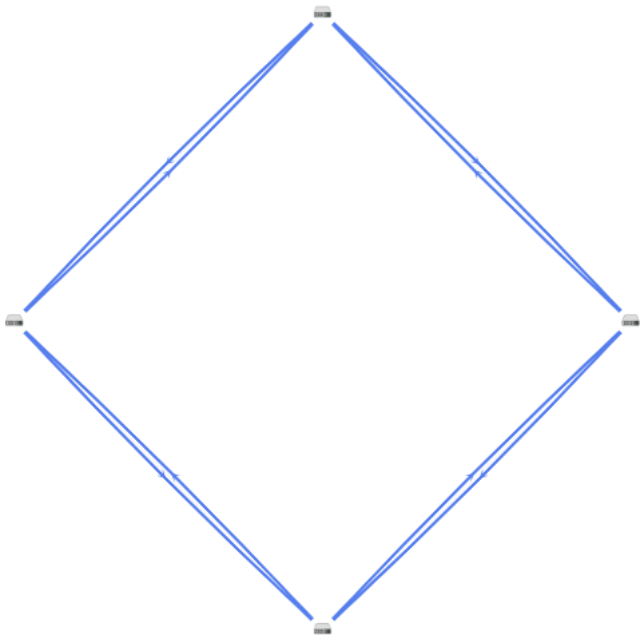
   - **Вручную** – вручную изменить взаимное расположение устройств CPE.
   - **Автоматически** – выбрать одно из значений в раскрывающемся списке, чтобы топология транспортного сервиса была сгенерирована автоматически:
     - **Физическая симуляция** – устройства CPE на схеме располагаются примерно в соответствии с их реальным расположением относительно друг-друга. Например:



- **Случайно** – устройства CPE располагаются случайным образом. Например:

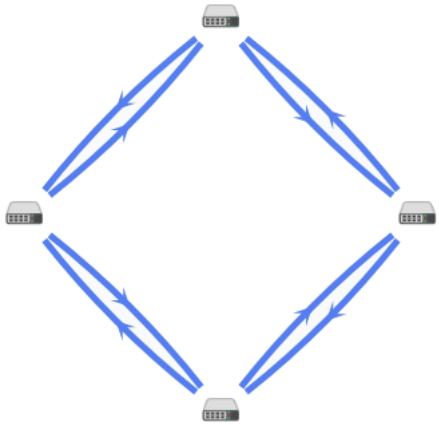


- **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо. Например:



- **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. При необходимости отобразить подписи к устройствам CPE, установите следующие флажки:

   - **Имя**.
   - **IP-адрес**.

   По умолчанию флажки сняты.

7. При необходимости отобразите туннели, используемые в сегменте из двух устройств CPE:

   a. Установите флажок **Сегменты**. По умолчанию флажок снят.

   b. Выберите устройства в раскрывающихся списках снизу или на схеме.

8. При необходимости отобразить окно с кнопками управления и дополнительной информацией об устройстве CPE или туннеле, нажмите на значок устройства или туннеля.

Перезагрузка M2M-сервиса

Перезагрузка M2M-сервиса может потребоваться в случае, если при его функционировании возникла проблема (например с сетевым подключением) или в текущую конфигурацию были внесены требующие перезагрузки изменения.

Чтобы перезагрузить M2M-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с M2M-сервисом и в раскрывающемся списке выберите **Перезагрузить**.

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

Откроется окно с сообщением об успешной перезагрузке M2M-сервиса. Контроллер SD-WAN добавит M2M-сервис на все устройства CPE, которые ранее использовались в этом сервисе.

Транспортный сервис IP multicast

IP multicast (далее также IP multicast-сервис) – транспортный сервис, в рамках которого внутри домена строится дерево распространения multicast-трафика для передачи данных нескольким интерфейсам-назначения от одного интерфейса-источника по протоколу IP. Это позволяет оптимизировать использование полосы пропускания и снизить нагрузку на сеть при наличии большого количества устройств.

Корнем дерева распространения multicast-трафика является сервисный интерфейс, к которому подключен источник трафика. Интерфейс-источник передает трафик на сервисные интерфейсы, к которым подключены подписчики (далее также интерфейсы-подписчики). Интерфейсы-подписчики могут подключаться к multicast-группам с адресом назначения из диапазона IP-адресов 224.0.0.0/4 по протоколу IGMPv2/v3.

Трафик передается через транспортный сервис IP multicast как Ethernet-кадры с IP payload без дополнительной инкапсуляции.

Создание IP multicast-сервиса

Перед созданием IP multicast-сервиса требуется выполнить следующие действия:

- активировать устройства CPE;
- создать сервисные интерфейсы для источника и подписчика трафика;
- создать QoS-правило.

Чтобы создать транспортный сервис IP multicast:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **IP multicast-сервисы**.

   Отобразится таблица IP multicast-сервисов.

4. Вверху страницы нажмите на кнопку **+ IP multicast-сервис**.

5. В открывшемся окне в поле **Имя** введите имя транспортного сервиса.

6. В раскрывающихся списках **Коммутатор-источник** и **Порт-источник** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как интерфейс-источник.

7. При необходимости отобразить в раскрывающемся списке **Порт-источник** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

8. В поле **IP запросчика** введите IP-адрес интерфейса-источника.

9. При необходимости добавьте резервный интерфейс-источник, через который трафик будет передаваться в случае выхода из строя основного интерфейса:

   a. Установите флажок **Резервный интерфейс**. По умолчанию флажок снят.

   b. В раскрывающихся списках **Резервный коммутатор** и **Резервный порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как резервный.

   c. При необходимости отобразить в раскрывающемся списке **Резервный порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

   d. При необходимости прекратить использование резервного сервисного интерфейса в случае восстановления основного, установите флажок **Автовозвращение при восстановлении**. По умолчанию флажок снят.

   e. При необходимости строить дерево распространения multicast-трафика не только на основном сервисном интерфейсе, но и на резервном, установите флажок **Резервное multicast-дерево**. Пакеты трафика отбрасываются на резервном сервисном интерфейсе, пока основной остается активным. По умолчанию флажок установлен.

10. Установите флажок **IGMP-прокси**, чтобы использовать прокси-сервер IGMP. Эта функция сохраняет передачу трафика на активные multicast-группы, к которым подключен как минимум один сервисный интерфейс-подписчик. По умолчанию флажок снят.

11. В раскрывающемся списке **QoS** выберите ранее созданное QoS-правило для интерфейса-источника.

12. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

13. В раскрывающихся списках **Коммутатор-подписчик** и **Порт-подписчик** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как интерфейс-подписчик.

14. При необходимости отобразить раскрывающемся списке **Порт-подписчик** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы, установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

15. Нажмите на кнопку **+ Добавить**, чтобы добавить сервисный интерфейс в транспортный сервис.

    Сервисный интерфейс отобразится внизу окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним. Вам нужно добавить как минимум один сервисный интерфейс, чтобы продолжить настройку IP multicast-сервиса.

16. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

17. В поле **IP-адрес** введите IP-адрес multicast-группы. Диапазон значений: от 224.0.0.0 до 239.255.255.255.

18. В раскрывающемся списке **Маска** выберите маску IP-адреса. Диапазон значений: от 24 до 32.

19. В раскрывающемся списке **GBR** выберите гарантированную скорость передачи (англ. Guaranteed Bit Rate, GBR) для multicast-группы.

20. Нажмите на кнопку **+ Добавить**, чтобы добавить multicast-группу в транспортный сервис.

    Multicast-группа отобразится внизу окна. Вы можете удалить multicast-группу, нажав на кнопку **Удалить** рядом с ней. Вам нужно добавить как минимум одну Multicast-группу, чтобы продолжить настройку IP multicast-сервиса.

21. Нажмите на кнопку **Создать**.

IP multicast-сервис будет создан и отобразится в таблице.

Изменение IP multicast-сервиса

Чтобы изменить IP multicast-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с IP multicast-сервисом и в раскрывающемся списке выберите одно из следующих значений:

   - **Изменить интерфейсы-источники**.
   - **Изменить интерфейсы-подписчики**.
   - **Изменить multicast-группы**.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию IP multicast-сервиса.

6. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с IP multicast-сервисом и в раскрывающемся списке выберите **Удалить**

5. При необходимости удалить добавленные в IP multicast-сервис сервисные интерфейсы в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

6. Нажмите на кнопку **Удалить**.

IP multicast-сервис будет удален и перестанет отображаться в таблице.

Просмотр статистики работы IP multicast-сервиса

Чтобы просмотреть статистику работы IP multicast-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с IP multicast-сервисом и в раскрывающемся списке выберите **Статистика**.

Откроется окно со статистикой IP multicast-сервиса.

Транспортный сервис L3 VPN

L3 VPN (далее также L3 VPN-сервис) – транспортный сервис, в рамках которого устанавливается безопасное соединение между удаленными сетями и/или площадками через общую физическую инфраструктуру по протоколу IP для обеспечения L3-маршрутизации.

L3 VPN-сервис логически изолирует передаваемый трафик создавая виртуальные частные сети.

При создании L3 VPN-сервиса вам нужно создать L3-интерфейсы поверх сервисных интерфейсов устройств CPE или M2M-сервисов для передачи трафика. Вы также можете указывать статические маршруты, чтобы вручную определять и настраивать маршрутизацию внутри VPN-сети.

Поддерживается топология Full-Mesh, в которой допускается взаимодействие между любыми сетями.

Создание L3 VPN-сервиса

Перед созданием L3 VPN-сервиса требуется выполнить следующие действия:

- активировать устройства CPE;
- создать ограничение (Manual-TE или пороговое);
- создать сервисные интерфейсы или транспортные сервисы M2M;
- создать QoS-правило;
- создать фильтр трафика.

Чтобы создать транспортный сервис L3 VPN:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **L3 VPN-сервисы**.

   Отобразится таблица L3 VPN-сервисов.

4. Вверху страницы нажмите на кнопку **+ L3 VPN-сервисы**.

5. В открывшемся окне в поле **Имя** введите имя транспортного сервиса.

6. В раскрывающемся списке **Ограничение** выберите ранее созданное ограничение, которое требуется добавить в транспортный сервис.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для равномерного распределения трафика по туннелям, что позволяет предотвращать перегрузку отдельных туннелей и избегать проблем с производительностью у пользователей:

   - **По потокам** – балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям. Это значение выбрано по умолчанию.
   - **По пакетам** – балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
   - **Широковещательный** – пакеты передаются одновременно во все туннели для исключения потерь.

8. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

9. В раскрывающемся списке **Режим** выберите тип L3-интерфейса:

   - **M2M-сервис** – создать L3-интерфейс поверх M2M-сервиса.
   - **Сервисный интерфейс** – создать L3-интерфейс поверх сервисного интерфейса.

10. Если в раскрывающемся списке **Режим** вы выбрали **M2M-сервис**, в раскрывающемся списке **M2M-сервис** выберите M2M-сервис, поверх которого требуется создать L3-интерфейс.

11. Если в раскрывающемся списке **Режим** вы выбрали **Сервисный интерфейс**, настройте сервисный интерфейс:

    a. В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, поверх которого требуется создать L3-интерфейс.

    b. В раскрывающемся списке **QoS** выберите ранее созданное QoS-правило для сервисного интерфейса.

    c. В раскрывающемся списке **Входящий фильтр** выберите ранее созданный фильтр трафика для сервисного интерфейса.

    d. При необходимости отобразить в раскрывающемся списке **Порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. установите флажок **Показать используемые интерфейсы**. По умолчанию флажок снят.

12. В поле **IP** введите IP-адрес L3-интерфейса.

13. В поле **Длина префикса** введите длину префикса L3-интерфейса. Диапазон значений: от 0 до 32.

14. В поле **MAC** введите MAC-адрес сервисного интерфейса. Вы можете сгенерировать MAC-адрес, нажав на кнопку **Сгенерировать**.

15. В поле **APR-возраст (сек.)** введите время в секундах, в течение которого записи будут храниться в ARP-таблице на контроллере SD-WAN. Диапазон значений: от 1 до 65 535. По умолчанию указано значение `200`.

16. Нажмите на кнопку **+ Добавить**, чтобы создать L3-интерфейс.

    L3-интерфейс отобразится внизу окна. Вы можете удалить L3-интерфейс, нажав на кнопку **Удалить** рядом с ним. Вам нужно добавить как минимум один L3-интерфейс, чтобы продолжить настройку L3 VPN-сервиса.

17. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

18. В поле **IP** введите IP-адрес узла или сети назначения.

19. В поле **Длина префикса** введите длину префикса узла назначения. Диапазон значений: от 0 до 32.

20. В раскрывающемся списке **SVI** выберите L3-интерфейс для отправки пакетов трафика на узел назначения.

21. В поле **Шлюз** введите IP-адрес шлюза для маршрутизации пакетов трафика.

22. В поле **Метрика** введите метрику статического маршрута. По умолчанию указано значение `0`.

23. Нажмите на кнопку **+ Добавить**, чтобы создать статический маршрут.

    Статический маршрут отобразится внизу окна. Вы можете удалить статический маршрут, нажав на кнопку **Удалить** рядом с ним.

24. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

25. Нажмите на кнопку **Создать**.

L3 VPN-сервис будет создан и отобразится в таблице.

Изменение L3 VPN-сервиса

Чтобы изменить L3 VPN-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с L3 VPN-сервисом и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию L3 VPN-сервиса.

6. Нажмите на кнопку **Сохранить**.

Перезагрузка L3 VPN-сервиса

Перезагрузка L3 VPN-сервиса может потребоваться в случае, если при его функционировании возникла проблема (например с сетевым подключением) или в текущую конфигурацию были внесены требующие перезагрузки изменения.

Чтобы перезагрузить L3 VPN-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с L3 VPN-сервисом и в раскрывающемся списке выберите **Перезагрузить**.

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

Откроется окно с сообщением об успешной перезагрузке L3 VPN-сервиса. Контроллер SD-WAN добавит L3 VPN-сервис на все устройства CPE, которые ранее использовались в этом сервисе.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с L3 VPN-сервисом и в раскрывающемся списке выберите **Удалить**.

5. При необходимости удалить добавленные в L3 VPN-сервис сервисные интерфейсы в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

6. Нажмите на кнопку **Удалить**.

L3 VPN-сервис будет удален и перестанет отображаться в таблице.

Просмотр ARP-таблицы L3 VPN-сервиса

Чтобы просмотреть ARP-таблицу L3 VPN-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с L3 VPN-сервисом и в раскрывающемся списке выберите **ARP-таблица**.

Откроется страница с ARP-таблицей L3 VPN-сервиса.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с L3 VPN-сервисом и в раскрывающемся списке выберите **ARP-таблица**.

   Откроется страница с ARP-таблицей L3 VPN-сервиса.

5. Вверху страницы нажмите на кнопку **+ Статическая ARP-запись**.

6. В открывшемся окне в раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, для которого требуется назначить соответствие между IP и MAC-адресом.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с L3 VPN-сервисом и в раскрывающемся списке выберите **ARP-таблица**.

   Откроется страница с ARP-таблицей L3 VPN-сервиса.

5. Нажмите на кнопку **Управление** рядом со статической записью и в раскрывающемся списке выберите **Изменить**.

6. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию статической записи в ARP-таблице L3 VPN-сервиса.

7. Нажмите на кнопку **Сохранить**.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с L3 VPN-сервисом и в раскрывающемся списке выберите **ARP-таблица**.

   Откроется страница с ARP-таблицей L3 VPN-сервиса.

5. Нажмите на кнопку **Управление** рядом со статической записью и в раскрывающемся списке выберите **Удалить**.

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

Статическая запись будет удалена и перестанет отображаться в ARP-таблице L3 VPN-сервиса.

Просмотр таблицы маршрутизации L3 VPN-сервиса

Чтобы просмотреть таблицу маршрутизации L3 VPN-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете 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** рядом с L3 VPN-сервисом и в раскрывающемся списке выберите **Таблица маршрутизации**.

Откроется окно с таблицей маршрутизации L3 VPN-сервиса.

Добавление транспортного сервиса в шаблоне CPE

Вы можете добавить транспортные сервисы в шаблоне CPE, после чего применить этот шаблон к устройствам. В этом случае поверх OpenFlow-интерфейсов, соответствующих LAN-интерфейсам устройств CPE, к которым применен шаблон, автоматически создаются сервисные интерфейсы для подключения к добавленным транспортным сервисам. Таким образом, вы избегаете необходимости в создании сервисных интерфейсов вручную и индивидуальном подключении каждого устройства CPE к транспортным сервисам.

Перед добавлением транспортного сервиса в конфигурации шаблона CPE требуется выполнить следующие действия:

- создать транспортный сервис в меню настройки контроллера SD-WAN;
- создать QoS-правило.

> Обратите внимание, что все указываемые вами параметры должны совпадать с ранее созданным транспортным сервисом. Например, вам нужно использовать то же самое имя и тип.

Чтобы добавить 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 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 **Транспортные сервисы**.

   Отобразится таблица транспортных сервисов.

4. Нажмите на кнопку **+ Транспортный сервис**.

5. В открывшемся окне в поле **Имя** введите имя транспортного сервиса.

6. В поле **Имя QoS** введите имя ранее созданного QoS-правила, которое используется в транспортном сервисе.

7. В раскрывающемся списке **Стадия** выберите состояние устройства CPE, в котором сервисный интерфейс требуется добавить в транспортный сервис:

   - **Перед активацией** – сервисный интерфейс добавляется в транспортный сервис перед активацией устройства CPE. Это значение выбрано по умолчанию.
   - **После активации** – сервисный интерфейс добавляется в транспортный сервис после активации устройства CPE.

8. В раскрывающемся списке **Тип** выберите одно из следующих значений:

   - **P2M**.

- **M2M**.
- **L3 VPN**.

9. В раскрывающемся списке **Инкапсуляция** выберите тип инкапсуляции на сервисном интерфейсе:
   - **Access** – это значение выбрано по умолчанию.
   - **VLAN**.
   - **Q-in-Q**.
10. Если в раскрывающемся списке **Инкапсуляция** вы выбрали **VLAN**, в поле **VLAN ID** введите внешнюю метку VLAN. Диапазон значений: от 1 до 4094.
11. Если в раскрывающемся списке **Инкапсуляция** вы выбрали **Q-in-Q**, выполните следующие действия:
    a. В поле **VLAN ID** введите внешнюю метку VLAN. Диапазон значений: от 1 до 4094.
    b. В поле **Внутренний VLAN ID** введите внутреннюю метку VLAN. Диапазон значений: от 1 до 4094.
12. Если в раскрывающемся списке **Тип** вы выбрали **P2M**, в раскрывающемся списке **Роль** выберите роль сервисного интерфейса:
    - **Leaf** – сервисный интерфейс, который может отправлять трафик только на интерфейсы с ролью Root.
    - **Root** – сервисный интерфейс, который может отправлять трафик на интерфейсы с любой ролью. Эту роль необходимо назначить как минимум одному сервисному интерфейсу.
13. Если в раскрывающемся списке **Тип** вы выбрали **L3VPN**, выполните следующие действия:
    a. В поле **IP-адрес** введите IP-адрес.
    b. В поле **Маска** введите маску сети. Диапазон значений: от 0 до 32.
14. Нажмите на кнопку **Создать**.

    Транспортный сервис будет добавлен и отобразится в таблице.
15. 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 конфигурации шаблона CPE:

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

   Отобразится таблица шаблонов CPE.
2. Нажмите на 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.

3. Выберите вкладку **Транспортные сервисы**.

   Отобразится таблица транспортных сервисов.

4. Нажмите на кнопку **Изменить** рядом с транспортным сервисом.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по добавлению транспортного сервиса в шаблоне CPE.

6. Нажмите на кнопку **Сохранить**.

Удаление в транспортного сервиса в шаблоне CPE

Удаленные в шаблоне CPE транспортные сервисы невозможно восстановить.

Чтобы удалить транспортный сервис в конфигурации шаблона CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на 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.

3. Выберите вкладку **Транспортные сервисы**.

   Отобразится таблица транспортных сервисов.

4. Нажмите на кнопку **Удалить** рядом с транспортным сервисом.

   Транспортный сервис будет удален и перестанет отображаться в таблице.

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

Сценарий: Направление трафика приложения в транспортный сервис

Kaspersky SD-WAN поддерживает распознавание трафика на уровне приложений. Эта функция может использоваться при определении политик качества обслуживания для выполнения следующих задач:

- Направление трафика приложения через определенный WAN-интерфейс устройства CPE, например, в соответствии со значениями SLA-метрик транспортных путей.
- Отбрасывание на устройстве CPE трафика определенного приложения, чтобы не передавать этот трафик в сеть SD-WAN.

В этом сценарии приводится последовательность действий, которые требуется выполнить, чтобы направить трафик одного или нескольких приложений в транспортный сервис. Перед выполнением этого сценария вам нужно создать транспортный сервис, в который будет направляться трафик приложения.

Сценарий направления трафика приложения в транспортный сервис состоит из следующих этапов:

1. **Создание правила классификации трафика**

   Правило классификации трафика используется для определения трафика указанного 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, создайте отдельное правило классификации трафика для каждого из них.

2. **Создание фильтра трафика**

   Фильтр трафика определяет, будет ли разрешена маршрутизация трафика приложения. При создании фильтра трафика вам нужно добавить в него правило классификации трафика для приложения или несколько правил.

3. **Создание ACL-интерфейса**

   ACL-интерфейс применяет фильтр к проходящему через него трафику. При создании ACL-интерфейса вам нужно выбрать фильтр трафика для приложения.

4. **Добавление ACL-интерфейса в транспортный сервис**

   Вам нужно изменить параметры транспортного сервиса и добавить ACL-интерфейс, через который в этот сервис будет поступать трафик приложения.

Зеркалирование трафика

Kaspersky SD-WAN поддерживает функциональность перенаправления и зеркалирования трафика из точек сбора в точку назначения в рамках отдельного TAP-сервиса. Точками сбора и назначения выступают сервисные интерфейсы. При этом точками сбора могут быть как отдельные сервисные интерфейсы, так и сервисные интерфейсы, используемые в транспортных сервисах. Точки сбора указываются при создании TAP-сервиса, а точку назначения необходимо создать заранее.

При перенаправлении входящий в точки сбора трафик передается в точку назначения, в то время как при зеркалировании передается его копия. Обратите внимание, что Kaspersky SD-WAN временно не поддерживает перенаправление и зеркалирование исходящего трафика.

Во время создания TAP-сервиса вы также можете указать правила классификации трафика, которые будут использоваться на точке назначения для отделения интересующих вас данных из общего потока.

Создание точки назначения трафика

Точка назначения – это сервисный интерфейс, на который будет передаваться трафик, поступающий в точки сбора, указанные при создании TAP-сервиса. Перед созданием точки назначения трафика требуется создать сервисный интерфейс.

Чтобы создать точку назначения трафика:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Точка назначения**, на которой отображается таблица точек назначения трафика.

4. Вверху страницы нажмите на кнопку **+ Точка назначения**.

5. В открывшемся окне в раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать в качестве точки 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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Точка назначения**, на которой отображается таблица точек назначения трафика.

4. Нажмите на кнопку **Удалить** рядом с точкой назначения трафика.

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

Точка назначения трафика будет удалена и перестанет отображаться в таблице.

Создание TAP-сервиса

Перед созданием TAP-сервиса требуется выполнить следующие действия:

- создать точку назначения трафика;
- создать сервисные интерфейсы, которые будут использоваться в качестве точек сбора трафика.

Обратите внимание, что вы можете применить одно или несколько правил классификации трафика к точке назначения трафика.

Чтобы создать TAP-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Точка назначения**, на которой отображается таблица точек назначения трафика.

4. Выберите вкладку **TAP-сервисы**.

   Отобразится таблица TAP-сервисов.

5. Вверху страницы нажмите на кнопку **+ TAP-сервис**.

6. При необходимости зеркалировать на точку назначения трафик, поступающий в точки сбора, установите флажок **Зеркалировать**. Когда флажок установлен, на точку назначения передается копия трафика, а когда снят – трафик перенаправляется. По умолчанию флажок снят.

7. В раскрывающемся списке **Режим балансировки** выберите режим балансировки для равномерного распределения трафика по туннелям, что позволяет предотвращать перегрузку отдельных туннелей и избегать проблем с производительностью у пользователей:

   - **По потокам** – балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям. Это значение выбрано по умолчанию.
   - **По пакетам** – балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
   - **Широковещательный** – пакеты передаются одновременно во все туннели для исключения потерь.

8. В раскрывающемся списке **Точка назначения** выберите точку назначения трафика.
9. В раскрывающемся списке **Тип точки сбора** выберите одно из следующих значений:

   - **Сервисный интерфейс** – отдельный сервисный интерфейс.
   - **Транспортный сервис** – сервисный интерфейс, используемый в транспортном сервисе.

10. 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.

11. В раскрывающемся списке **Точки сбора** выберите сервисные интерфейсы, которые требуется использовать в качестве точек сбора трафика.
12. Нажмите на кнопку **Далее** и выберите ранее созданные правила классификации трафика для точки назначения.
13. Нажмите на кнопку **Создать**.

TAP-сервис будет создан и отобразится в таблице.

Изменение TAP-сервиса

Чтобы изменить TAP-сервис:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Точка назначения**, на которой отображается таблица точек назначения трафика.

4. Выберите вкладку **TAP-сервисы**.

   Отобразится таблица TAP-сервисов.

5. Нажмите на кнопку **Управление** рядом с TAP-сервисом и в раскрывающемся списке выберите **Изменить**.

6. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию TAP-сервиса.

7. Нажмите на кнопку **Сохранить**.

Просмотр статистики работы TAP-сервиса

Чтобы просмотреть статистику работы TAP-сервиса:

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

   Откроется страница управления ресурсами. По умолчанию будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Точка назначения**, на которой отображается таблица точек назначения трафика.

4. Выберите вкладку **TAP-сервисы**.

   Отобразится таблица TAP-сервисов.

5. Нажмите на кнопку **Управление** рядом с TAP-сервисом и в раскрывающемся списке выберите **Статистика**.

Откроется окно со статистикой работы TAP-сервиса.

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 будет выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN и SDN.

2. Нажмите на кнопку **Управление** → **Меню конфигурации** рядом с контроллером SD-WAN.

   Откроется меню настройки контроллера. По умолчанию вы перейдете в раздел **Узлы контроллера**, в котором отображается таблица узлов контроллера.

3. Перейдите в раздел **TAP-сервисы**.

   По умолчанию выбрана вкладка **Точка назначения**, на которой отображается таблица точек назначения трафика.

4. Выберите вкладку **TAP-сервисы**.

   Отобразится таблица TAP-сервисов.

5. Нажмите на кнопку **Управление** рядом с TAP-сервисом и в раскрывающемся списке выберите **Удалить**.

6. При необходимости удалить добавленные в TAP-сервис сервисные интерфейсы в открывшемся окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

7. Нажмите на кнопку **Удалить**.

TAP-сервис будет удален и перестанет отображаться в таблице.

Планировщик задач

Kaspersky SD-WAN поддерживает отложенный запуск задач с помощью планировщика. Вы можете использовать теги, чтобы сгруппировать устройства CPE для отложенного запуска задач на этих устройствах.

Поддерживаются следующие типы отложенных задач:

- Запуск скриптов на устройствах CPE. Вам нужно предварительно добавить скрипты, которые вы хотите запустить, в шаблон CPE.
- Обновление прошивок на устройствах CPE. Вам нужно предварительно загрузить прошивку, которую вы хотите установить, в веб-интерфейс оркестратора.

Когда вы назначаете отложенное выполнение задачи, Kaspersky SD-WAN использует часовой пояс хоста оркестратора. 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 – 18:00.

Во время настройки отложенного выполнения задач учитывайте следующие особенности:

- Допускается 10-секундная погрешность во времени при выполнении задачи.
- Если задача не выполняется из-за недоступности оркестратора в назначенное время, она отображается со статусом *Ошибка*.
- При наличии нескольких задач по конфигурированию устройства CPE они выполняются параллельно. Если оркестратор не может выполнить все задачи параллельно, они выполняются в порядке создания.
- Если вы удалите шаблон CPE, с которым связаны задачи, они также будут удалены.
- Если вы удалите устройство CPE, с которым связаны задачи, они также будут удалены.
- При попытке удалить связанный с задачами скрипт вам потребуется дополнительно подтвердить это действие.

Вы можете вручную выполнить отложенные задачи, которые еще не были выполнены.

Создание отложенной задачи

Чтобы создать отложенную задачу:

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

   Отобразится таблица отложенных задач.

2. Вверху страницы нажмите на кнопку **Отложенная задача**.

3. В открывшемся окне в раскрывающемся списке **Тип** выберите одно из следующих значений:

   - **Запуск скрипта** – задача по отложенному запуску скрипта.
   - **Отложенное обновление прошивки** – задача по отложенному обновлению прошивки.

4. Укажите параметры отложенной задачи. Описание параметров отложенных задач см. в следующих инструкциях:

   - Отложенный запуск скрипта.
   - Обновление прошивки.

5. Нажмите на кнопку **Создать**.

Отложенная задача будет создана и отобразится в таблице.

Выполнение отложенной задачи вручную

Чтобы вручную выполнить отложенную задачу:

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

   Отобразится таблица отложенных задач.

2. При необходимости выполните отдельную отложенную задачу:

   a. Нажмите на отложенную задачу.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

   b. Вверху области настройки в блоке **Действия** нажмите на кнопку **Выполнить сейчас**.

3. При необходимости выполните несколько отложенных задач одновременно:

   a. Установите флажки рядом с отложенными задачами.

   b. Вверху в раскрывающемся списке **Действия** выберите **Выполнить сейчас**.

4. В открывшемся окне подтверждения нажмите на кнопку **Выполнить сейчас**.

Одна или несколько отложенных задач будут выполнены и их статус в таблице изменится на *Выполнено*.

Удаление отложенной задачи

Удаленные отложенные задачи невозможно восстановить.

Чтобы удалить отложенную задачу:

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

   Отобразится таблица отложенных задач.

2. При необходимости удалите отдельную отложенную задачу:

   a. Нажмите на отложенную задачу.

   В нижней части страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на значок развертывания ⌃.

   b. Вверху области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

3. При необходимости удалите несколько отложенных задач одновременно:

   a. Установите флажки рядом с отложенными задачами.

   b. Вверху в раскрывающемся списке **Действия** выберите **Удалить**.

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

Одна или несколько отложенных задач будут удалены и перестанут отображаться в таблице.

Глоссарий

Customer Premise Equipment (CPE)

Телекоммуникационное оборудование, включая виртуальные машины, находящееся на клиентской площадке. Используется для подключения клиентской площадки к сети SD-WAN, установки туннелей 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.

DSCP-значения

6-битные значения, которые определяют приоритет пакетов трафика и требуемый тип обслуживания. Они используются в сочетании с классами трафика для предоставления соответствующего приоритета и полосы пропускания критически важному сетевому трафику, например трафику приложений, которые обеспечивают передачу аудио-видео сигнала.

Physical Network Function (PNF)

Заранее развернутые сетевые функции, которые в готовом виде загружается в веб-интерфейс оркестратора. Оркестратор может осуществлять дальнейшую конфигурацию PNF.

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.

Universal CPE (uCPE)

Устройства CPE с дополнительной поддержкой развертывания виртуальных сетевых функций. Обратите внимание, что устройство должно иметь достаточно аппаратных ресурсов для того, чтобы не задействовать ЦОД или облако во время предоставления VNF.

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 каналов, 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).

Virtual Network Function Manager (VNFM)

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

Контроллер SD-WAN

Централизованно управляет наложенной сетью и сетевыми устройствами в соответствии с топологией сервисной цепочки по протоколу OpenFlow. Развертывается как виртуальная или физическая сетевая функция.

Оркестратор

Контролирует инфраструктуру решения, выполняет функции оркестратора NFV (NFVO), а также управляет сетевыми сервисами и распределенными VNFM. Может управляться 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 SD-WAN.

Тенант

Логическая сущность, в рамках которой разворачивается 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 устанавливают туннели со всеми устройствами в сети, включая другие шлюзы, таким образом обеспечивая связность между всеми устройствами и контроллером SD-WAN. Вы можете установить несколько шлюзов 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.

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, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы о развертывании 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:

- отправить запрос в Службу технической поддержки Kaspersky SD-WAN по адресу sdwan-support@kaspersky.com;
- 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.

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 – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

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.

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 – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

Zabbix – зарегистрированный товарный знак Zabbix SIA.