kaspersky

Kaspersky SD-WAN

Содержание

О Kaspersky SD-WAN

Kaspersky SD-WAN используется, чтобы строить программно-определяемые распределенные сети (англ. Software Defined WAN, далее сети SD-WAN) для маршрутизации трафика по каналам передачи данных с применением технологии SDN (Software Defined Networking). Основной особенностью таких сетей является возможность автоматического определения наиболее эффективных маршрутов передачи трафика.

Технология SDN подразумевает разделение плоскости управления сетью (англ. control plane) и плоскости передачи данных (англ. data plane). Плоскость управления сетью состоит из контроллера SD-WAN и оркестратора. Она контролирует передачу пакетов трафика по сети через устройства Customer Premise Equipment (далее устройства CPE, устройства), которые установлены на клиентских площадках и образуют плоскость передачи данных. Альтернативным методом управления сетью является API.

Виртуализация сетевых функций (англ. Network Function Virtualization, NFV) выполняется в соответствии со стандартами, указанными в спецификации NFV MANO (NFV Management and Network Orchestration) Европейского института по стандартизации в области телекоммуникаций (англ. European Telecommunications Standards Institute, ETSI).

Решение предназначено для операторов связи (англ. service providers), а также организаций, имеющих крупную филиальную сеть, и заменяет стандартные маршрутизаторы в распределенных сетях. Процесс развертывания не зависит от транспортных технологий, используемых в вашей сети. Поддерживается использование нескольких туннелей для передачи трафика с учетом требований приложений к пропускной способности и качеству обслуживания.

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

- Интеллектуальное управление трафиком.
- Автоматическая настройка устройств CPE. Эта функциональность позволяет задействовать меньше специалистов при развертывании устройств на площадках.
- Централизованное управление инфраструктурой сети через веб-интерфейс оркестратора. Например, вы можете использовать веб-интерфейс, чтобы настраивать устройства CPE и туннели.
- Постоянный мониторинг топологии сети и автоматическое реагирование на ее изменение. Например, вы можете настроить передачу трафика по резервному туннелю, если при работе основного туннеля возникает сбой.
- Автоматическое реагирование сети на изменения качества обслуживания в каналах передачи данных, чтобы соответствовать требованиям различных приложений, используемых в сети.

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

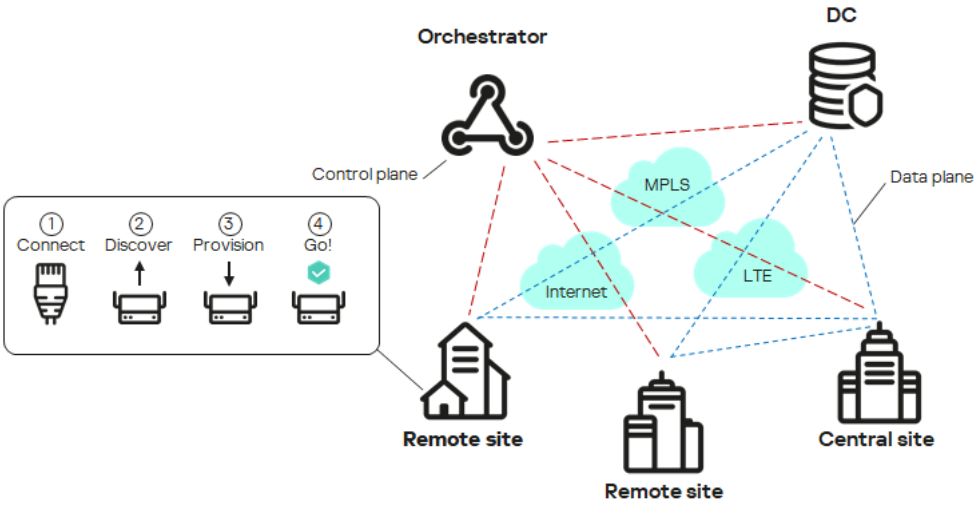


Схема сети SD-WAN

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:

- Docker-контейнеры для развертывания решения:
  - knaas-ctl;
  - knaas-orc;
  - knaas-www;
  - knass-vnfm;
  - knaas-vnfm-proxy.
- Прошивка для установки устройств CPE и последующей работы с ними.
- 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

В решение входят следующие программные модули:

- Оркестратор, который входит в backend-часть решения.
- Веб-интерфейса оркестратора, который входит во frontend-часть решения.
- База данных оркестратора (MongoDB версии 5.0.7).
- VNFM.
- Веб-сервер NGINX, который используется для балансировки запросов HTTP и HTTPS к VNFM и предоставления веб-прокси устройствам CPE и VNF.
- Резидентная база данных Redis версии 6.2.7.
- Контроллер SD-WAN

Модули разворачиваются в виде Docker-контейнеров для независимой установки и масштабирования. При необходимости вы можете предоставлять дополнительные ресурсы каждому модулю (ядра процессора, оперативная память) и распределять их между несколькими серверами, чтобы увеличить общую производительность.

Компоненты Kaspersky SD-WAN могут быть развернуты на нескольких физических серверах или виртуальных машинах (далее также ВМ). Поддерживаются платформы виртуализации KVM и VMware. Вам нужно обеспечить наличие серверов или виртуальных машин для установки Kaspersky SD-WAN, внешней системы мониторинга Zabbix версии 5.0.26, а также контроллера SD-WAN.

Существует два варианта развертывания контроллера:

- В виде VNF в облачной платформе OpenStack (релиз Xena). Узлы контроллера размещаются на вычислительных узлах.
- В виде PNF на отдельных виртуальных машинах.

Перед развертыванием Kaspersky SD-WAN убедитесь, что ваша сетевая инфраструктура соответствует следующим аппаратным и программным требованиям.

Аппаратные требования

В таблицах ниже представлены требования к аппаратным ресурсам. Обратите внимание, что эти требования зависят от количества управляемых устройств CPE, которые используются в экземпляре SD-WAN. В таблицах указаны типовые значения, поэтому если требуется рассчитать точные требования для вашей схемы развертывания, обратитесь в техническую поддержку "Лаборатории Касперского".

Аппаратные требования к серверам или виртуальным машинам для развертывания оркестратора

Устройства CPE	Ядра процессора	Оперативная память, ГБ	Дисковое пространство, ГБ	Сетевые адаптеры	Виртуальные машины
до 50	8	8	105	2	3
до 100	8	10	110	2	3
до 250	8	12	125	2	3
до 500	8	16	150	2	3
до 1000	10	24	200	2	3

до 5000	12	32	600	2	3
до 10000	16	64	1100	2	5

Аппаратные требования к серверам или виртуальным машинам для развертывания остальных компонентов решения

Устройства CPE	Ядра процессора	Оперативная память, ГБ	Дисковое пространство, ГБ	Сетевые адаптеры	Контейнеры
Контроллер SD-WAN					
до 50	4	8	64	2	3
до 100	6	8	64	2	3
до 250	8	16	64	2	3
до 500	8	16	64	2	6
до 1000	8	16	64	2	12
до 5000	8	16	64	2	60
до 10000	8	16	64	2	120
VNFM					
до 50	4	8	20	2	3
до 100	4	8	20	2	3
до 250	4	8	20	2	3
до 500	4	8	20	2	3
до 1000	4	10	20	2	3
до 5000	4	12	20	2	3
до 10000	4	16	20	2	3
Система мониторинга Zabbix					
до 50	4	8	100	2	3
до 100	4	10	200	2	3
до 250	6	12	350	2	3
до 500	8	24	600	2	3
до 1000	10	32	1100	2	3
до 5000	12	64	5100	2	3
до 10000	16	128	10100	2	3

Если требуется подключить более 250 устройств CPE, развертываются дополнительные кластеры контроллеров SD-WAN.

Более подробную информацию об аппаратных требованиях к системе мониторинга Zabbix можно получить из официальной документации решения Zabbix.

При развертывании решения настраивается офлайн-карта (англ. offline map). Вам необходимо учитывать следующие требования к свободному дисковому пространству:

- Офлайн-карта (central-fed-district-latest.osm.pbf) занимает около 100 ГБ.

- Данные для геокодинга занимают около 10 ГБ.

Мы рекомендуем учитывать возможность использования переподписки на этапе планирования ресурсов для развертывания экземпляра SD-WAN. Максимальный коэффициент переподписки, доступный, когда вы развертываете контейнеры, составляет 3. Коэффициент определяется следующими характеристиками экземпляра SD-WAN:

- количество используемых устройств CPE;
- частота изменений состояния сети;
- скорость передачи трафика;
- размер передаваемых пакетов трафика.

Требования к каналам

Поддерживаются следующие каналы:

- транспортные сети MPLS;
- широкополосные каналы для подключения к интернету;
- арендуемые линии связи;
- беспроводные подключения, в том числе 3G, 4G, LTE и 5G;
- спутниковые каналы связи.

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").

Поддерживаемые браузеры

Вы можете использовать следующие браузеры, чтобы работать с веб-интерфейсом оркестратора:

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

Требования к устройствам CPE

Kaspersky SD-WAN поддерживает использование следующих устройств:

- 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.

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), а также было выключено шифрование трафика.

Протестированные модели устройств CPE (услуга L3 VPN)

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

Более подробная информация о характеристиках устройств CPE, которые вы можете использовать в Kaspersky SD-WAN, содержится на официальной странице решения.

Требования к общему хранилищу (shared storage)

Kaspersky SD-WAN использует общее хранилище (англ. shared storage, далее также хранилище), чтобы обеспечить отказоустойчивость. В этом хранилище содержатся следующие папки с необходимыми оркестратору данными:

- backups – резервные копии конфигураций VNF и PNF;
- firmware – прошивки устройств CPE;

- images – образы VNF;
- vnf_configs – файлы, которые могут использоваться скриптами при конфигурации VNF;
- vnf_descriptions – VNF-дескрипторы.

Мы рекомендуем использовать собственное общее хранилище. Существуют следующие требования к развертываемому общему хранилищу:

- Поддержка одновременной записи и чтения с нескольких хостов.
- Рекомендованный 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: не менее 1 ГБит/с, рекомендуется использовать 10-гигабитный Ethernet или 8-гигабитный FC (Fiber Channel).
- Поддерживаемое значение IOPS (input/output operations per second): не менее 250, рекомендуется не менее 400.
- Тип хранилища:
  - NFS.
  - iSCSI.
  - FC.
  - CephFS.
- Хранилище должно быть монтировано.
- Поддержка сохранения работоспособности при перезагрузке хоста.

Что нового

В Kaspersky SD-WAN 2.1 появились следующие возможности и доработки:

- Поддержан протокол динамической маршрутизации OSPF.
- Поддержаны дополнительные сценарии соединения между устройствами CPE в случае расположения шлюза SD-WAN за NAT.
- Поддержаны дополнительные сценарии работы устройств CPE с одновременным использованием каналов Internet и MPLS.
- Поддержана настройка IP-адресов контроллера на WAN-интерфейсах устройств CPE.
- Поддержана работа с картой топологии SD-WAN без подключения к сети.
- Добавлена ротация токена и пароля для устройств CPE.
- Поддержано шифрование данных мониторинга при их отправке вне туннеля SD-WAN.

Архитектура решения

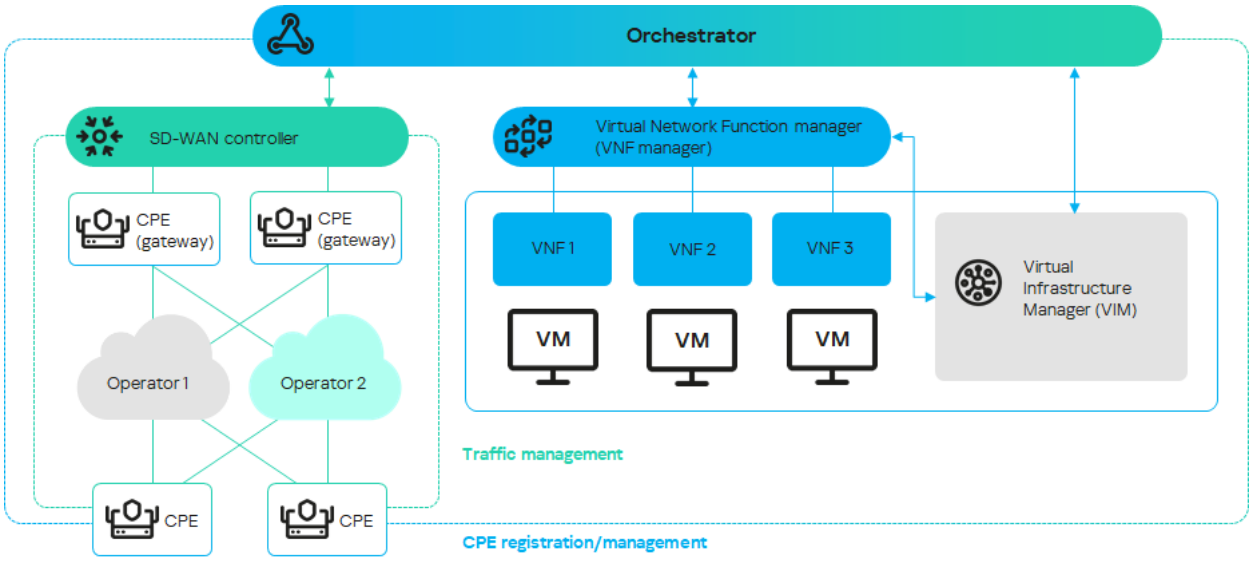
Kaspersky SD-WAN содержит следующие компоненты:

- **Оркестратор** – обеспечивает управление инфраструктурой решения, в том числе устройствами CPE, через графический веб-интерфейс. Оркестратор может управлять несколькими экземплярами SD-WAN.
- **Контроллер SD-WAN** – централизованно управляет устройствами CPE по протоколу OpenFlow, а также наложенной сетью, на основании которой вы можете создавать транспортных сервисы.
- **Устройства CPE** – образуют SDN-фабрику в виде наложенной сети. Устройствам CPE можно назначить роль *шлюзов SD-WAN*. В этом случае до них автоматически строятся туннели от всех остальных устройств, которым назначена роль стандартного CPE. Если вы планируете использовать шлюзы SD-WAN в топологии сети, мы рекомендуем устанавливать их в нескольких экземплярах для обеспечения отказоустойчивости.
- **Менеджер виртуальных сетевых функций (англ. Virtual Network Function Manager, далее также VNFM)** – обеспечивает конфигурацию виртуальных сетевых функций (англ. Virtual Network Functions, далее также VNF) и устройств CPE.

Все компоненты решения разворачиваются в центрах обработки данных (далее также ЦОДы), за исключением устройств CPE, которые устанавливаются на удаленных площадках. Если вы разворачиваете экземпляр SD-WAN с использованием VNF, в архитектуру решения могут входить следующие дополнительные компоненты:

- **Контроллер SDN** – обеспечивает управление и конфигурацию аппаратных и программных коммутаторов в ЦОД. Использование этого компонента не обязательно.
- **VIM** – обеспечивает управление вычислительными и сетевыми ресурсами, а также ресурсами хранения. Все эти ресурсы необходимы для работы VNF.

Kaspersky SD-WAN имеет распределенную микросервисную архитектуру, которая разворачивается в виде Docker-контейнеров (см. рисунок ниже). Контроллер SD-WAN может состоять из одного узла или кластера из трех/пяти узлов. Узлы кластера контроллера являются отдельными виртуальными машинами и могут запускаться на разных аппаратных серверах, чтобы обеспечить отказоустойчивость.



Архитектура Kaspersky SD-WAN

Резервирование и отказоустойчивость

Отказоустойчивость обеспечивает последовательную и непрерывную передачу трафика по сети SD-WAN, а также работу сетевых сервисов. Ее уровень повышается за счет применения механизмов резервирования и аварийного переключения на разных уровнях инфраструктуры сети, например, когда вы создаете резервные сервисные интерфейсы.

Если сеть является отказоустойчивой, она может сохранить свою работоспособность как при возникновении небольших проблем, так и серьезных аварий, связанных с функционированием центральных компонентов, таких как маршрутизаторы, туннели и центры обработки данных. Когда один из компонентов перестанет выполнять назначенные ему функции, его место занимает резервный компонент такого же типа. Например, вы можете построить резервный туннель, на который трафик будет передан, если основной туннель будет недоступен.

Отказоустойчивость упрощает балансировку нагрузки между несколькими туннелями, позволяя оптимизировать использование полосы пропускания трафика и избежать перегрузок. В этом случае ни один из существующих туннелей не может стать узким местом (англ. bottleneck) в топологии сети.

Kaspersky SD-WAN обеспечивает непрерывную работу в случае возникновения следующих видов сбоев:

- отказ одного из центральных компонентов, например оркестратора, шлюза или контроллера SD-WAN;
- отказ или перегрузка каналов передачи данных между центральными компонентами при их георезервировании, когда компоненты сети размещаются на географически разнесенных площадках, чтобы сделать хранение данных более надежным;
- отказ или перегрузка каналов передачи данных между устройствами CPE и шлюзами SD-WAN.

Резервирование центральных компонентов решения

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

Схема развертывания N+1 подразумевает, что вместе с активным компонентом развертывается один резервный компонент. Если активный компонент выходит из строя, резервный компонент мгновенно занимает его место, обеспечивая непрерывность работы.

Схема развертывания 2N+1 является расширенной версией N+1 и отличается тем, что имеет дополнительный уровень резервирования. В рамках этой схемы активный компонент состоит из двух наборов. Они синхронизированы между собой, и один может занять место другого, если возникает неполадка. При этом также развертывается один дополнительный резервный компонент. 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.

Схемы резервирования компонентов решения

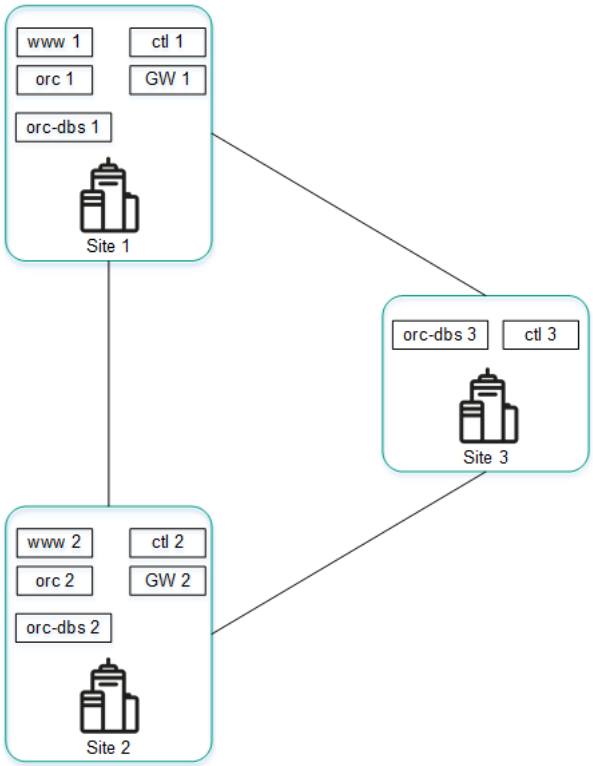
Компонент	Схема резервирования	Используемый протокол
Оркестратор	N+1	REST
Веб-интерфейс оркестратора	N+1	REST
База данных оркестратора	2N+1	MONGODB
Контроллер SD-WAN и его база данных	2N+1	OPENFLOW (TLS)

Шлюз SD-WAN	N+1	GENEVE

Пример размещения компонентов решения в географически разнесенных ЦОД представлен на рисунке ниже. На всех последующих рисунках используются одинаковые 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 в разных ЦОД. Каждый из узлов находится в активном состоянии. Вы можете выбрать узел, к которому направляются запросы, с помощью виртуального IP-адреса или службы DNS.

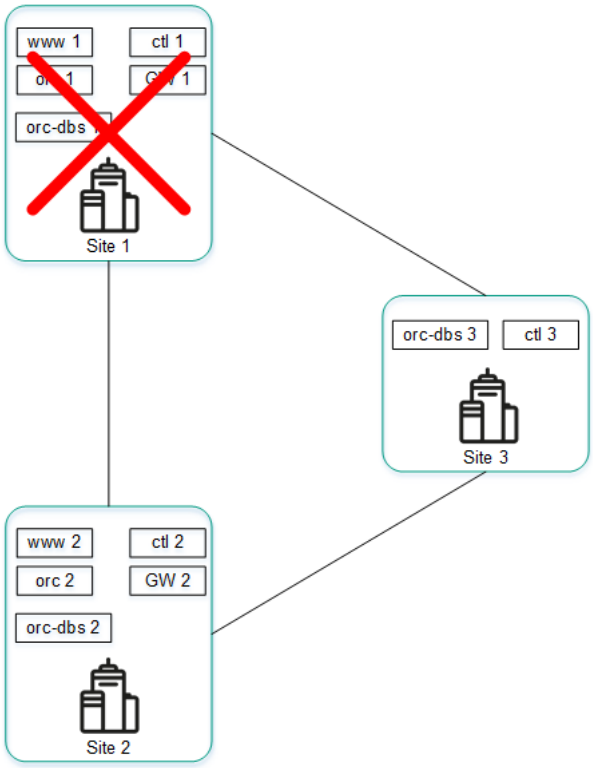


Размещение компонентов решения в географически разнесенных ЦОД

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 служебными пакетами (англ. heartbeats).

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:

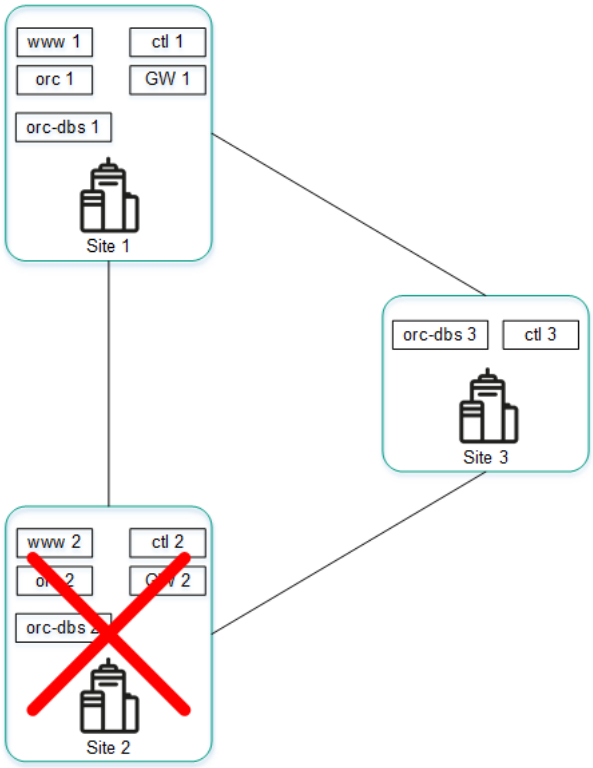
a. Узел orc-dbs 2 и узел-арбитр orc-dbs 3 теряют связь с узлом orc-dbs 1, после чего выбирают новый основной узел.

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

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

d. 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.



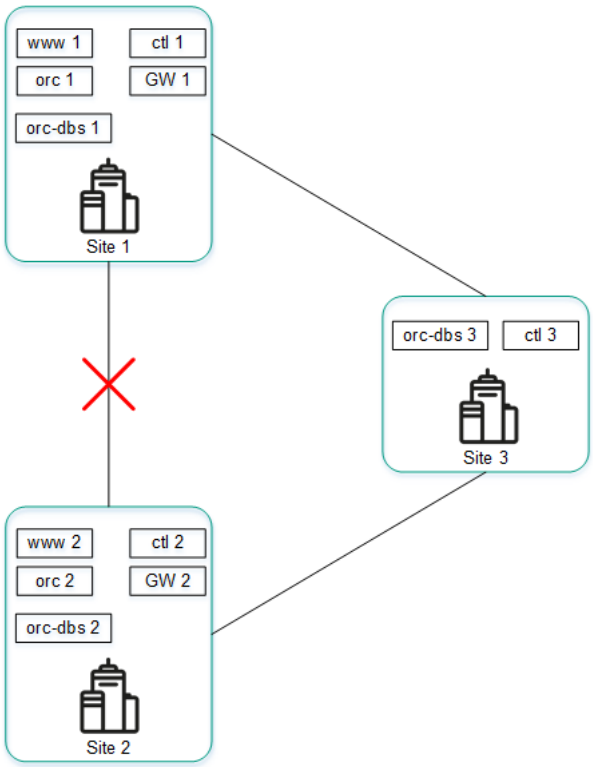
Авария на площадке 2

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

a. 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.

b. 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:

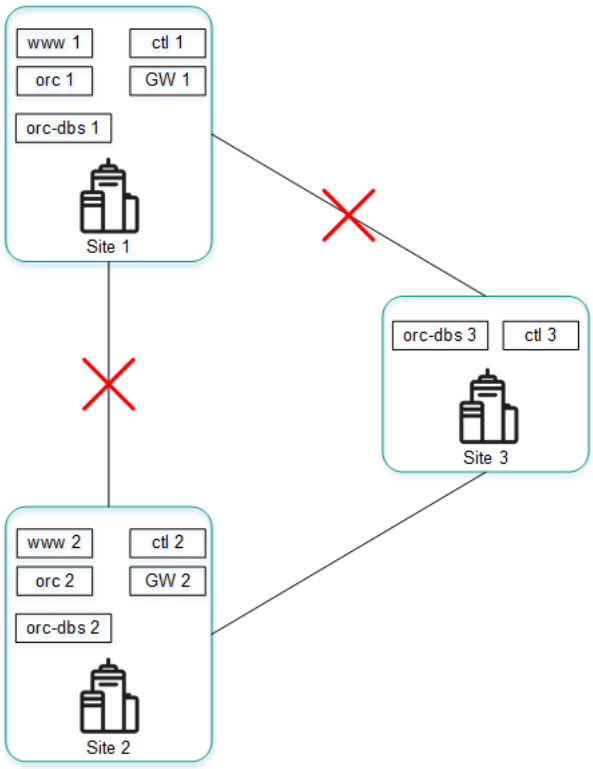
a. Узел orc-dbs 1 теряет связь с узлом orc-dbs 2.

b. Узел orc-dbs 1 остается основным узлом, потому что узел-арбитр orc-dbs 3 видит, что обе площадки работают в штатном режиме.

c. Узел ctl 1 теряет связь с узлом ctl 2.

d. 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, происходит следующие события:

a. Узел orc-dbs 1 теряет связь с узлом orc-dbs 2.

b. 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.

c. Узел ctl 1 теряет связь с узлом ctl 2.

d. Узел ctl 2 становится основным узлом и сообщает оркестратору о своей роли, потому что узел-арбитр ctl 3 видит, что площадка 1 недоступна.

Резервирование каналов передачи данных между устройствами CPE

Kaspersky SD-WAN обеспечивает защиту от перерывов связи между устройствами CPE, одновременно используя все доступные каналы передачи данных, например интернет-каналы или LTE-каналы.

Режим Active/Active

В этом режиме все WAN-интерфейсы устройств CPE находятся в активном состоянии и передают трафик пользователей.

Контроллер SD-WAN обеспечивает балансировку трафика с использованием от 2 до 16 транспортных путей (англ. multipathing). *Балансировка* равномерно распределяет трафик по туннелям, что позволяет предотвратить перегрузку отдельных туннелей и возникновение проблем с производительностью у пользователей. Поддерживается три режима балансировки:

- По потокам (англ. per flow) с учетом информации на уровнях L2–L4. В этом режиме доступно два типа балансировки:
  - 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 передачи данных.

Режим Active/Standby

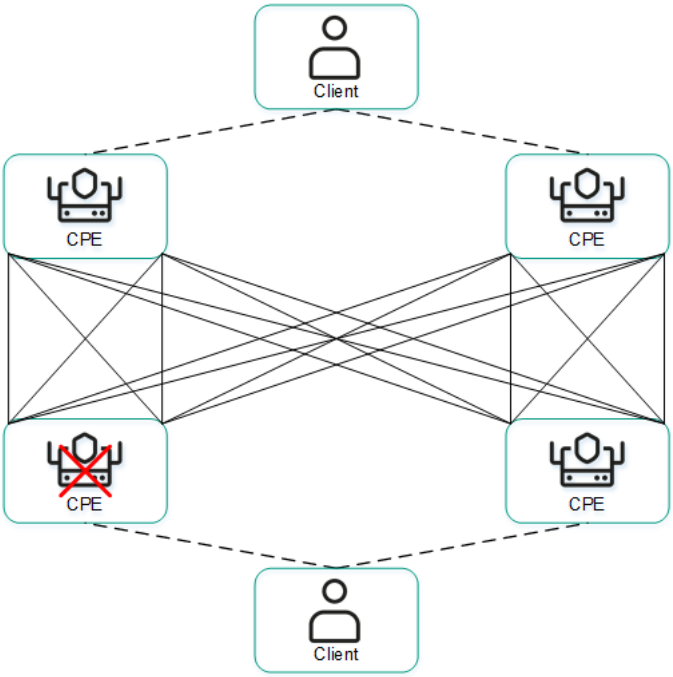
В этом режиме вам нужно выбрать основной и резервный транспортный путь для передачи трафика. Балансировка при этом не используется. На устройство CPE заранее загружаются правила использования резервного WAN-интерфейса в ситуации, когда путь через основной WAN-интерфейс становится недоступным. В этом случае при нарушении работы основного транспортного пути не производится переписывание правил коммутации пакетов, и устройство отправляет их через резервный интерфейс.

Вы можете настроить резервирование на уровне транспортных сервисов. При создании транспортного сервиса указываются резервные сервисные интерфейсы (англ. reserve SI) на выбранном устройстве CPE или на другом устройстве. Мы рекомендуем создавать основной и резервный сервисные интерфейсы на разных устройствах. Трафик переключается на резервный сервисный интерфейс, если основной сервисный интерфейс недоступен.

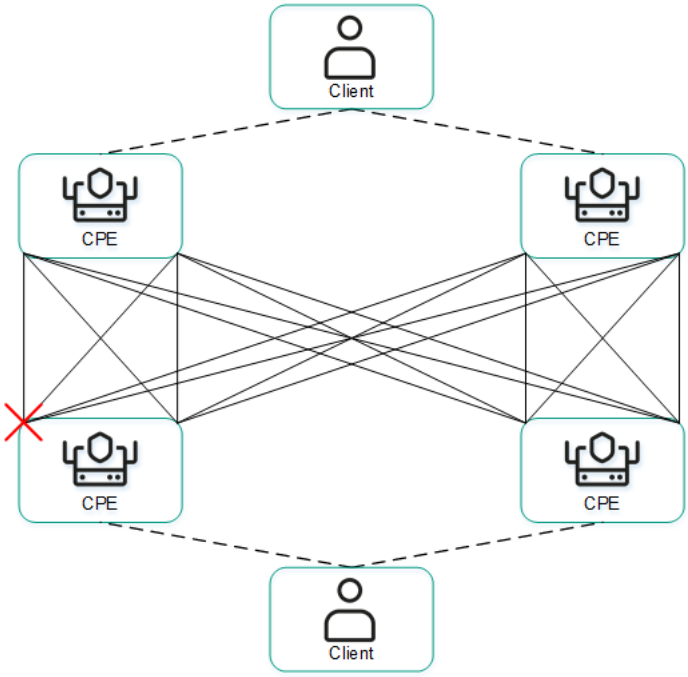
Решение поддерживает создание резервных сервисных интерфейсов для всех типов транспортных сервисов уровня L2.

На рисунках ниже представлены основные примеры перерывов связи между устройствами CPE:

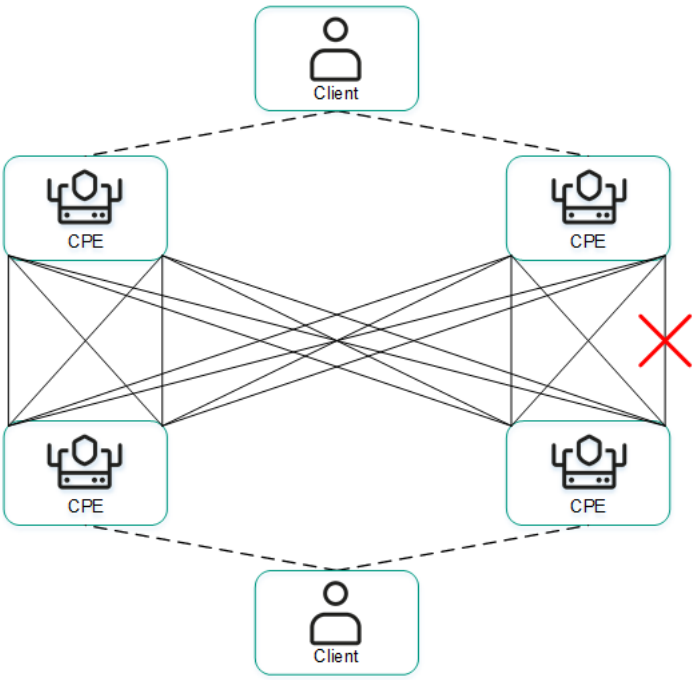
- Выход из строя одного из устройств CPE.



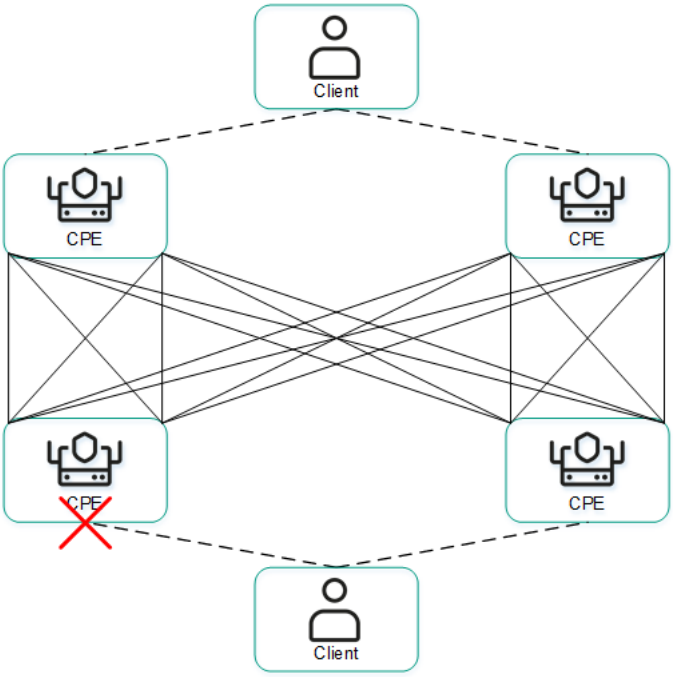
- Выход из строя WAN-интерфейса одного из устройств CPE.



- Выход из строя связности между двумя устройствами CPE.



- Выход из строя LAN-интерфейса одного из устройств CPE.



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).

Протоколы для передачи управляющего трафика

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, чтобы идентифицировать устройства CPE во время их установки и регистрации:

- Обнаружение устройства CPE с помощью идентификатора DPID.
- Отложенная регистрация. Вы можете выбрать, в каком состоянии находится устройство CPE после успешной регистрации – *Активировано* или *Деактивировано*. Деактивированное устройство CPE нужно активировать вручную, убедившись, что оно установлено на площадке.
- Двухфакторная аутентификация – клиент получает ключ, который требуется ввести на устройстве CPE, чтобы активировать его.

Во время регистрации устройство CPE проверяет подлинность сертификата оркестратора, после чего отправляет ему свой идентификатор DPID и токен. Оркестратор проверяет их наличие в базе данных и в случае успеха отправляет устройству информацию, необходимую для подключения к сети, а также конфигурацию. Затем устройство устанавливает подключение с контроллером SD-WAN, который в свою очередь программирует его поведение для последующей обработки трафика.

Если переданный идентификатор DPID отсутствует в инвентаризационной базе, устройство CPE отображается со статусом *Неизвестно* и не подключается к сети SD-WAN.

Использование VNF

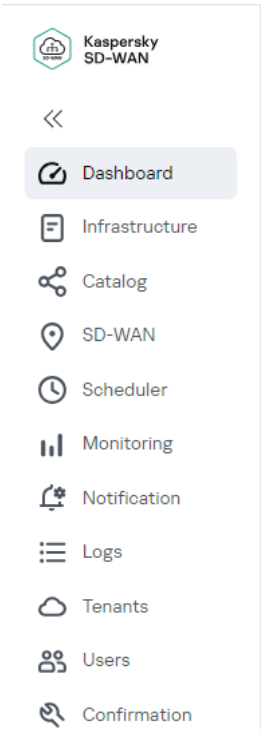
Вы можете обеспечить дополнительный уровень безопасности с помощью **VNF**, разворачиваемых в ЦОД и/или на uCPE. Например, трафик может быть направлен от устройства CPE к VNF, которая выполняет функцию сетевого экрана или прокси-сервера. VNF могут выполнять следующие функции защиты сети SD-WAN:

> Сетевые функции, реализуемые в виде виртуальных машин на обычных компьютерных платформах COTS (Commercial Off The Shelf).

- 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 URL- и веб-контента;
- система защиты от утечек конфиденциальной информации DLP (Data Loss Prevention);
- веб-прокси Secure Web Proxy.

Интерфейс решения

Управление Kaspersky SD-WAN осуществляется через веб-интерфейс оркестратора. Вы можете использовать разделы, которые отображаются в меню (см. рисунок ниже), чтобы настроить отдельные компоненты решения. Когда вы переходите в один из разделов, отображается дополнительное меню с его содержимым.



Меню Kaspersky SD-WAN

Меню содержит следующие разделы:

- **Обозреватель** ( ) – в этом разделе вы можете просмотреть информацию о текущем состоянии компонентов решения, таких как устройства CPE, VNF и PNF.
- **Инфраструктура** ( ) – в этом разделе вы можете управлять инфраструктурой сети, например создать домены, а также добавить центры обработки данных и VIM. Кроме того, здесь отображаются все доступные вам контроллеры SD-WAN.
- **Каталог** ( ) – в этом разделе вы можете выполнять следующие действия в зависимости от вашей роли:
  - администратор платформы может загружать пакеты VNF/PNF и создавать шаблоны сетевых сервисов;
  - администратор тенанта может создавать сетевые сервисы.
- **SD-WAN** ( ) – в этом разделе вы можете управлять устройствами CPE, экземплярами SD-WAN, UNI, а также прошивками и сертификатами устройств.
- **Планировщик** ( ) – в этом разделе вы можете управлять отложенными задачами.
- **Журнал** ( ) – в этом разделе вы можете просмотреть журналы работы различных компонентов решения. Например, здесь отображаются внесенные пользователями изменения в конфигурацию устройств CPE.
- **Тенанты** ( ) – в этом разделе вы можете создать тенантов и предоставить им различные компоненты решения, например устройства CPE, VIM и UNI. Здесь вы также можете подключиться к веб-интерфейсу оркестратора тенанта в качестве администратора.

- **Пользователи** ( ) – в этом разделе вы можете создать пользователей, группы пользователей и права доступа, а также настроить доменную аутентификацию.

- **Подтверждение** ( ) – в этом разделе вы можете управлять запросами на подтверждение.

Когда вы переходите в один из разделов, меню отображается в свернутом виде. Вам нужно навести курсор мыши на значок одного из разделов, чтобы снова развернуть меню. Вы можете нажать на кнопку разворачивания », чтобы выключить функцию автоматического сворачивания меню.

Аутентификация в Kaspersky SD-WAN

Чтобы аутентифицироваться в Kaspersky SD-WAN:

1. В адресной строке браузера введите IP-адрес или имя сервера Kaspersky SD-WAN.

2. На открывшейся странице аутентификации введите ваше имя пользователя и пароль. Пароль должен содержать как минимум один прописной символ A-Z, строчные символы, цифры, а также специальные символы. Длина пароля: от 8 до 50 символов.

3. Нажмите на кнопку **Войти**.

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

Установка и сброс страницы по умолчанию

Страница по умолчанию – это раздел или подраздел веб-интерфейса оркестратора (включая меню настройки контроллера SD-WAN), который автоматически отображается после вашей аутентификации.

Чтобы установить или сбросить страницу по умолчанию:

1. Перейдите в раздел или подраздел веб-интерфейса оркестратора, который требуется установить как страницу по умолчанию.

2. Внизу меню нажмите на кнопку настройки и в раскрывающемся списке выберите **Сделать страницей по умолчанию**.

   Вверху отобразится сообщение `Страница по умолчанию установлена`.

3. При необходимости сбросить страницу по умолчанию нажмите на кнопку настройки и в раскрывающемся списке выберите **Сбросить страницу по умолчанию**.

   Вверху отобразится сообщение `Страница по умолчанию сброшена`. Теперь страницей по умолчанию является раздел **Обозреватель**.

Переключение между светлой и темной темой

Чтобы переключиться между светлой и темной темой веб-интерфейса оркестратора,

внизу меню нажмите на кнопку настройки и в раскрывающемся списке выберите одно из следующих значений:

- **Темная тема**.
- **Светлая тема**.

Ограничение продолжительности пользовательской сессии при бездействии

По умолчанию после аутентификации в веб-интерфейсе оркестратора вы можете бездействовать на протяжении 3600 секунд, после чего пользовательская сессия прекращается. Вы можете вручную увеличить или уменьшить время возможного бездействия.

Чтобы указать время, по прошествии которого ваша пользовательская сессия прекращается при бездействии:

1. Внизу меню нажмите на кнопку настройки и в раскрывающемся списке выберите **Время истечения сессии**.
2. В открывшемся окне введите время в секундах, по истечении которого требуется прекратить сессию при бездействии. Диапазон значений: от 60 до 86 400. По умолчанию указано значение `3600`.
3. Нажмите на кнопку **Сохранить**.

Просмотр активных пользовательских сессий

Вы можете просматривать список пользователей, которые использовали вашу учетную запись, чтобы аутентифицироваться в веб-интерфейсе оркестратора.

Чтобы просмотреть активные пользовательские сессии:

1. Внизу меню нажмите на кнопку настройки и в раскрывающемся списке выберите **Активные сессии**.

   Отобразится таблица активных пользовательских сессий.
2. При необходимости прекратить отдельную пользовательскую сессию нажмите на кнопку **Закончить сессию** рядом с этой сессией.
3. При необходимости прекратите несколько пользовательских сессий одновременно:

   a. Установите флажки рядом с сессиями.

   b. Вверху страницы нажмите на кнопку **Действия** и в раскрывающемся списке выберите **Закончить сессию**.

Настройка 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, чтобы проводить мониторинг контейнеров, а также быстрее восстанавливать их работу, когда возникают сбои.

При открытии журнала в верхней части страницы, а также рядом с каждым Docker-контейнером отображаются следующие кнопки для выбора уровня детализации:

- **ТРАССИРОВКА** – включать в журналы наиболее полную информацию, включая отладочные операторы (англ. debug statements), для расширенного поиска и устранения проблем.
- **ОТЛАДКА** – включать в журналы детализированную информацию, включая значения переменных и записи о вызовах функций, для поиска и устранения проблем, а также понимания принципов функционирования контейнера.
- **ИНФОРМАЦИЯ** – включать в журналы общую информацию для понимания принципов функционирования контейнера и поиска важных событий. Этот уровень детализации выбран по умолчанию для всех контейнеров.
- **ПРЕДУПРЕЖДЕНИЕ** – включать в журналы записи об ошибках или событиях, которые не требуют незамедлительного вмешательства со стороны пользователя, но могут скомпрометировать работу контейнера.
- **ОШИБКА** – включать в журналы записи об ошибках или исключениях которые могут скомпрометировать работу контейнера. Такие записи зачастую требуют незамедлительного вмешательства со стороны пользователя.

Чтобы настроить уровень детализации журналов Docker-контейнеров:

1. Внизу меню нажмите на кнопку настройки и в раскрывающемся списке выберите **Параметры журналов**.

   Откроется таблица Docker-контейнеров.

2. Выберите уровень детализации журналов Docker-контейнеров:

   - Если вы хотите настроить уровень детализации журналов всех Docker-контейнеров, в блоке **Глобальный уровень журналирования** нажмите на соответствующую кнопку.
   - Если вы хотите настроить уровень детализации журналов отдельного Docker-контейнера, в столбце **Уровень журналирования** нажмите на соответствующую кнопку.

Переход к API оркестратора

Чтобы перейти к API оркестратора,

внизу меню нажмите на кнопку перехода к API.

Откроется список API-команд, доступных для управления оркестратором.

Изменение языка веб-интерфейса оркестратора

Веб-интерфейс оркестратора поддерживает английский и русский язык.

Чтобы изменить язык веб-интерфейса оркестратора,

внизу меню нажмите на одну из следующих кнопок:

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

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.

Пользовательские 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".

Управление доменами Kaspersky SD-WAN

В Kaspersky SD-WAN *домены* – это логические группы сетевых ресурсов, которые могут состоять из одного или нескольких центров обработки данных. Между доменами распределяются сетевые ресурсы, обеспечивающие функционирование решения.

Создание домена

Чтобы создать домен:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Вверху 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**. Теперь в этот домен можно добавлять центры обработки данных, чтобы объединить их в одну логическую группу.

Изменение домена

Чтобы изменить домен:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. В панели **Ресурсы** выберите вкладку **Домен**.

   Отобразится список доменов.

3. Нажмите на кнопку настройки рядом с доменом и в раскрывающемся списке выберите **Изменить**.

4. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию домена.

5. Нажмите на кнопку **Сохранить**.

Удаление домена

Удаленные домены невозможно восстановить.

Чтобы удалить домен:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. В панели **Ресурсы** выберите вкладку **Домен**.

   Отобразится список доменов.

3. Нажмите на кнопку настройки рядом с доменом и в раскрывающемся списке выберите **Удалить**.

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

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

Управление центрами обработки данных

Центральные компоненты Kaspersky SD-WAN, за исключением устройств CPE, размещаются в центрах обработки данных.

Центр обработки данных – это централизованная площадка, на которой располагаются компьютерные системы и связанные с ними компоненты, например серверы, системы хранения информации, сетевые устройства, а также системы безопасности. Они используются для хранения, распределения и передачи больших объемов данных. Ресурсы ЦОД предоставляются экземплярам SD-WAN.

Обратите внимание, что при добавлении ЦОД вам нужно указать веб-адрес развернутого **VNFM**.

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

Добавление центра обработки данных

Перед добавлением центра обработки данных требуется создать домен.

Чтобы добавить центр обработки данных:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Вверху страницы нажмите на кнопку **+ Центр обработки данных**.

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

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

5. В раскрывающемся списке **Домен** выберите домен, в который требуется добавить ЦОД.

6. В поле **VNFM URL** введите веб-адрес менеджера виртуальных функций. ЦОД использует введенный адрес, чтобы подключиться к VNFM и получить доступ к находящимся под его управлением VNF. Вы можете убедиться в доступности VNFM, нажав на кнопку **Проверить соединение**.

7. При необходимости в поле **Адрес** введите адрес ЦОД.

8. Нажмите на кнопку **Создать**.

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

Миграция центра обработка данных

Когда вы мигрируете центр обработки данных, он переносится из одного домена Kaspersky SD-WAN в другой. Если несколько центров обработки данных объединяются в одной локации, это снижает стоимость аренды и количество выполняемых операций, а также улучшает общую производительность.

Когда офисы вашей организации или индивидуальные пользователи сталкиваются с задержками при работе с сетью SD-WAN, миграция центра обработки данных в локацию, которая расположена ближе к офисам или пользователям, обеспечивает более надежную связь.

Вы также можете переместить центр обработки данных в более экономически выгодную локацию, в которой, например, допускается использование облачных сервисов или совместная аренда оборудования с другими организациями.

Чтобы мигрировать центр обработки данных:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. В панели **Ресурсы** выберите вкладку **Центр обработки данных**.

   Отобразится список центров обработки данных.

3. Нажмите на кнопку настройки рядом с центром обработки данных и в раскрывающемся списке выберите **Мигрировать**.

4. В открывшемся окне выберите домен, в который требуется мигрировать центр обработки данных.

5. Нажмите на кнопку **Мигрировать**.

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

Изменение центра обработки данных

Чтобы изменить центр обработки данных:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. В панели **Ресурсы** выберите вкладку **Центр обработки данных**.

   Отобразится список центров обработки данных.

3. Нажмите на кнопку настройки рядом с центром обработки данных и в раскрывающемся списке выберите **Изменить**.

4. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по добавлению центра обработки данных.

5. Нажмите на кнопку **Сохранить**.

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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. В панели **Ресурсы** выберите вкладку **Центр обработки данных**.

   Отобразится список центров обработки данных.

3. Нажмите на кнопку настройки рядом с центром обработки данных и в раскрывающемся списке выберите **Удалить**.

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

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

Управление VIM

Перед развертыванием VNF в центре обработки данных необходимо добавить как минимум один VIM. В Kaspersky SD-WAN используется VIM облачной платформы OpenStack, предоставляющий все ее ключевые возможности, например виртуализацию сети, управление виртуальными машинами и распределение нагрузки.

Настройка VIM

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.

Вы можете настроить VIM в центре обработки данных или шаблоне uCPE. Когда вы изменяете параметры VIM в шаблоне uCPE, указанные параметры применяются ко всем устройствам, использующим этот шаблон. Для настройки VIM используйте следующие инструкции:

- **Настройка VIM в центре обработки данных**.

Чтобы настроить VIM в центре обработки данных:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Вверху страницы нажмите на кнопку **+ VIM**.

3. В открывшемся окне в раскрывающихся списках **Домен** и **Центр обработки данных** выберите домен и ЦОД, в котором развернут VIM.

4. В поле **Имя** введите имя VIM.

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

6. В поле **Порт** введите номер порта для подключения оркестратора к сервису идентификации VIM. По умолчанию указано значение `5000`.

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

   - **http** – это значение выбрано по умолчанию.
   - **https**.

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

9. При необходимости измените дополнительные параметры аутентификации оркестратора в облачной платформе OpenStack:

   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.

10. В раскрывающемся списке **За NAT** выберите, находится ли VIM за NAT (Network Address Translation):

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

11. При необходимости укажите коэффициенты переподписки физических ресурсов:

    a. В поле **Переподписка ЦП** введите коэффициент переподписки процессорных ядер. 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 учитывайте, 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.

12. При необходимости 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.

13. В раскрывающемся списке **Кластер SDN** выберите SDN-кластер, к которому подключен OpenStack, или значение **Отсутствует**, если OpenStack не подключен к SDN-кластеру.

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

15. 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.

16. Если для управления вы используете сеть с типом сегментации VLAN, в поле **Физическая VLAN-сеть** введите идентификатор VLAN ID.

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

    a. При необходимости 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.

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

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

b. При необходимости 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, которая используется, чтобы изолировать и защищать трафик 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, включена функция Port sercurity или нет. *Функция Port security* повышает уровень безопасности сети на уровне Ethernet-портов коммутаторов. Она 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. Вы можете выбрать одно из следующих значений:

- **Включено**.
- **Выключено**.

f. В поле **Разрешить CIDR** введите адрес разрешенной подсети для сети управления.

19. Нажмите на кнопку **Создать**.

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

- Настройка VIM в шаблоне uCPE.

Чтобы настроить VIM в шаблоне uCPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

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** – это значение выбрано по умолчанию.
   - **https**.

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

7. При необходимости укажите дополнительные параметры аутентификации оркестратора в облачной платформе OpenStack:

   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 ID.

9. В раскрывающемся списке **За NAT** выберите, находится ли VIM за NAT (Network Address Translation):

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

10. При необходимости укажите коэффициенты переподписки физических ресурсов:

    a. В поле **Переподписка ЦП** введите коэффициент переподписки процессорных ядер. 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 учитывайте, 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 планируется использовать на VIM. Этот параметр позволяет оркестратору отслеживать количество сегментов, доступных для использования. Диапазон значений: от 0 до 4094.

12. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Просмотр использования VIM

Вы можете просматривать, какие вычислительные ресурсы использует VIM, чтобы более эффективно управлять сетевой инфраструктурой и при необходимости оптимизировать ее использование.

Чтобы просмотреть использование VIM:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Выберите вкладку **Вычислительные ресурсы**.

   Отобразится таблица VIM.

3. Нажмите на кнопку **Управление** рядом с VIM и в раскрывающемся списке выберите **Показать использование**.

Откроется окно с информацией о том, насколько VIM использует следующие вычислительные ресурсы:

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

Изменение VIM

Чтобы изменить VIM:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Выберите вкладку **Вычислительные ресурсы**.

   Отобразится таблица VIM.

3. Нажмите на кнопку **Управление** рядом с VIM и в раскрывающемся списке выберите **Изменить**.

4. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по добавлению VIM.

5. Нажмите на кнопку **Сохранить**.

Удаление VIM

Удаленные VIM невозможно восстановить.

Чтобы удалить VIM:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Выберите вкладку **Вычислительные ресурсы**.

   Отобразится таблица VIM.

3. Нажмите на кнопку **Управление** рядом с VIM и в раскрывающемся списке выберите **Удалить**.

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

VIM будет удален и перестанет отображаться в таблице.

Управление подсетями

Подсети позволяют разделить вашу сеть на сегменты, а также организовать эффективное управление IP-адресами и сетевыми ресурсами за счет отделения управляющего трафика от пользовательского.

При создании подсети вы добавляете диапазон IP-адресов. Входящие в этот диапазон адреса автоматически назначаются устройствам в подсети. Вам нужно добавить как минимум один диапазон IP-адресов для каждого центра обработки данных, используемого в вашей организации.

Создание подсети

Чтобы создать подсеть:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Вверху страницы нажмите на кнопку **+ Подсеть**.

3. В открывшемся окне в раскрывающихся списках **Домен** и **Центр обработки данных** выберите домен и ЦОД, к которому относится подсеть.

4. В поле **Имя** введите имя подсети.

5. В раскрывающемся списке **Версия IP** выберите версию IP-адресов, которые использует подсеть:

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

6. В поле **CIDR** введите IP-адрес и маску подсети. Формат значения: <IP-адрес>/<маска подсети>, например 192.168.2.0/24.

7. В поле **Шлюз** введите IP-адрес шлюза по умолчанию, который сетевые устройства в подсети должны использовать, чтобы взаимодействовать с другими сетями.

8. В блоке **Диапазон IP** нажмите на кнопку **+ Добавить**, чтобы добавить диапазон IP-адресов, и в отобразившихся полях введите начальное и конечное значение диапазона. IP-адреса из диапазона назначаются сетевым устройствам в подсети. Вы можете добавить несколько диапазонов.

   Вам нужно добавить как минимум один диапазон IP-адресов для каждого центра обработки данных, используемого в вашей организации.

9. В блоке **DNS** нажмите на кнопку **+ Добавить**, чтобы добавить DNS-сервер, и в отобразившемся поле введите IP-адрес сервера. Сетевые устройства получают IP-адрес DNS-сервера вместе с IP-адресами из диапазона. Наличие DNS-серверов позволяет сетевым устройствам преобразовывать доменные имена в IP-адреса и таким образом поддерживать зависящие от DNS приложения, такие как браузеры и электронная почта. Вы можете добавить несколько серверов.

10. В блоке **Статические маршруты** нажмите на кнопку **+ Добавить**, чтобы добавить статический маршрут, и в отобразившемся поле введите маршрут. Сетевые устройства получают статический маршрут вместе с IP-адресами из диапазона. Наличие статических маршрутов позволяет управлять маршрутизацией трафика между подсетями, чтобы выполнять такие задачи, как оптимизация передачи трафика,

маршрутизация определенного вида трафика по указанному назначению, а также установка соединения между двумя удаленным площадками. Вы можете добавить несколько маршрутов.

11. Нажмите на кнопку **Создать**.

Подсеть будет создана отобразится в таблице на вкладке **IPAM**.

Изменение подсети

Чтобы изменить подсеть:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Выберите вкладку **IPAM**.

   Отобразится таблица подсетей.

3. Нажмите на кнопку **Управление** рядом с подсетью и в раскрывающемся списке выберите **Изменить**.

4. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию подсети.

5. Нажмите на кнопку **Сохранить**.

Удаление подсети

Удаленные подсети невозможно восстановить.

Чтобы удалить подсети:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Выберите вкладку **IPAM**.

   Отобразится таблица подсетей.

3. Нажмите на кнопку **Управление** рядом с подсетью и в раскрывающемся списке выберите **Удалить**.

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

Подсеть будет удалена и перестанет отображаться в таблице.

Просмотр журналов

Журналы используются, чтобы обнаруживать возникающие при работе решения ошибки, а также осуществлять техническую поддержку. Kaspersky SD-WAN не осуществляет отправку журналов за пределы периметра информационной инфраструктуры вашей организации – все файлы журналов хранятся локально.

Чтобы просмотреть записи журнала:

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

   Откроется страница управления журналами.

2. В панели **Центры обработки данных** выберите центр обработки данных.

3. В панели **Ресурсы** выберите компонент решения.

4. В панели **Журналы** выберите одну из следующих вкладок, чтобы отобразить записи журнала определенного типа:

   - **Задачи** – задачи, выполняемые пользователем, например запись о добавлении VIM.
   - **События** – события, происходящие во время работы решения, например подключение туннеля.
   - **Сервисные запросы** – сервисные запросы к определенным компонентам решения, например запрос на регистрацию устройства CPE.

   По умолчанию в журнале отображаются задачи, события и сервисные запросы за весь период и с любыми статусами. Вы можете отобразить только нужные вам записи с помощью фильтров вверху страницы.

Сервисные запросы

Сервисные запросы (англ. service requests) – это задачи, которые выполняются во время работы компонентов решения и создаются автоматически в результате действий пользователей. Например, когда пользователь применяет шаблон CPE к устройству, создается соответствующий сервисный запрос. Вы можете использовать сервисные запросы, чтобы проводить мониторинг выполняемых операций.

В Kaspersky SD-WAN сервисные запросы создаются на уровне тенантов, устройств CPE и экземпляров SD-WAN. Для просмотра сервисных запросов используйте следующие инструкции:

- Просмотр сервисных запросов тенанта.

  Чтобы просмотреть сервисные запросы тенанта:

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

     Отобразится страница управления тенантами.

  2. В блоке **Тенанты** выберите тенанта.

     Сервисные запросы отобразятся в блоке **Сервисные запросы**.

     Вы можете открыть пошаговый журнал выполнения сервисного запроса с подробной информацией о каждом шаге, нажав на имя запроса. Журнал содержит информацию о шагах, на которых произошли ошибки, а также подробное описание самих ошибок.

- Просмотр сервисных запросов устройства CPE.

  Чтобы просмотреть сервисные запросы устройства CPE:

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

     По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

  2. Нажмите на устройство CPE.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

  3. Выберите вкладку **Сервисные запросы**.

     Отобразится таблица сервисных запросов. Вы можете открыть пошаговый журнал выполнения сервисного запроса с подробной информацией о каждом шаге, нажав на идентификатор запроса. Журнал содержит информацию о шагах, на которых произошли ошибки, а также подробное описание самих ошибок.

- Просмотр сервисных запросов экземпляра SD-WAN.

Чтобы просмотреть сервисные запросы экземпляра SD-WAN:

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

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Сервисные запросы**.

Отобразится таблица сервисных запросов. Вы можете открыть пошаговый журнал выполнения сервисного запроса с подробной информацией о каждом шаге, нажав на идентификатор запроса. Журнал содержит информацию о шагах, на которых произошли ошибки, а также подробное описание самих ошибок.

При необходимости вы можете удалить сервисный запрос, созданный на уровне устройства CPE или экземпляра SD-WAN, чтобы прекратить выполнение связанной с этим запросом операции. Для этого используйте следующие инструкции:

- Удаление сервисного запроса устройства CPE.

  Удаленные сервисные запросы невозможно восстановить.

  Чтобы удалить сервисный запрос устройства CPE:

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

     По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

  2. Нажмите на устройство CPE.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

  3. Выберите вкладку **Сервисные запросы**.

     Отобразится таблица сервисных запросов.

  4. Удалите сервисные запросы:

     - Если вы хотите удалить отдельный сервисный запрос, нажмите на кнопку **Удалить** рядом с этим запросом.

       Сервисный запрос будет удален и перестанет отображаться в таблице.

     - Если вы хотите удалить все сервисные запросы, вверху области настройки в блоке **Действия** нажмите на кнопку **Удалить все сервисные запросы**.

       Все сервисные запросы будут удалены и перестанут отображаться в таблице.

- Удаление сервисного запроса экземпляра SD-WAN.

Удаленные сервисные запросы невозможно восстановить.

Чтобы удалить сервисный запрос экземпляра SD-WAN:

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

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Сервисные запросы**.

   Отобразится таблица сервисных запросов.

4. Удалите сервисные запросы:

   - Если вы хотите удалить отдельный сервисный запрос, нажмите на кнопку **Удалить** рядом с этим запросом.

     Сервисный запрос будет удален и перестанет отображаться в таблице.

   - Если вы хотите удалить все сервисные запросы, вверху области настройки в блоке **Действия** нажмите на кнопку **Удалить все сервисные запросы**.

     Все сервисные запросы будут удалены и перестанут отображаться в таблице.

Управление сетевыми сервисами

Сетевые сервисы передают трафик по сети и применяют к нему сетевые функции, такие как WAN-оптимизация, шейпинг и идентификация трафика, а также защита данных. Несколько сетевых сервисов объединяются в *сервисную цепочку* для последовательного применения входящих в эти сервисы функций к трафику при передаче на место назначения.

Вы можете создать шаблон сетевого сервиса для упрощенного развертывания этого сервиса в рамках тенантов.

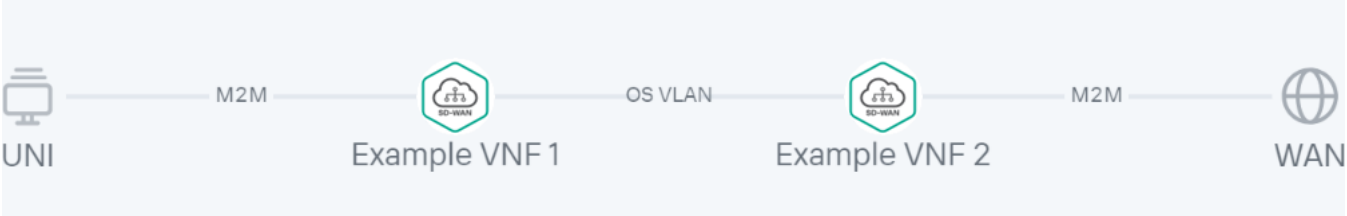
Основным сетевым сервисом, отвечающим за развертывание и функционирование Kaspersky SD-WAN, является *сервис SD-WAN*. Этот сервис создается в первую очередь и в него помещаются компоненты, которые входят в плоскость управления сетью. В рамках каждого экземпляра SD-WAN развернут как минимум один сервис SD-WAN.

Для создания сетевых сервисов и их шаблонов используется графический конструктор. Он позволяет наглядно построить топологию сервиса, помещая в нее следующие компоненты:

- Сетевые компоненты, такие как VNF и PNF.
- Соединения (англ. links), такие как транспортные сервисы P2P, P2M и M2M, а также OpenStack-соединения, например общая сеть OS 2 Shared.
- UNI и WAN-интерфейсы.

К сетевым компонентам и интерфейсам подключаются соединения, в результате чего строится топология сетевого сервиса. Вы можете связать отдельно созданные сетевые сервисы, поместив общий сетевой сервис в (англ. shared network service, shared NS) в их топологию.

Пример построенной топологии сетевого сервиса представлен на рисунке ниже.



Пример построенной топологии сетевого сервиса

Роли пользователей и действия с сетевыми сервисами

В таблице ниже представлены роли пользователей и действия, которые они могут выполнять при работе с сетевыми сервисами. Если вам назначена роль администратора платформы, вы можете аутентифицироваться в веб-интерфейсе тенанта как администратор и выполнить требуемые действия.

Роли пользователей и доступные им действия с сетевыми сервисами

Действие	Администратор платформы	Администратор тенанта
Создание шаблонов сетевых сервисов.	✓	–
Загрузка пакета VNF/PNF в каталог.	✓	–
Настройка сетевых компонентов.	✓	✓

Создание и развертывание сетевых сервисов.	–	✓
Просмотр развернутых сетевых сервисов.	✓	✓

Загрузка пакета VNF или PNF в оркестратор

Пакеты VNF и *PNF* являются ZIP-архивами, содержащими компоненты, необходимые для развертывания виртуальных и физических сетевых функций, а также для последующего управления этими функциями. Вы можете подготовить собственный пакет сетевой функции и определить, как интерфейс управления этой функцией будет выглядеть в веб-интерфейсе оркестратора.

Каждый пакет имеет следующую структуру:

- Файлы-дескрипторы VNFD (Virtual Network Function descriptor) или PNFD (Physical Network Function descriptor) в формате YAML. Это конфигурационные файлы, которые предоставляют детальную информацию о сетевой функции, и содержат спецификации, такие как требования к развертыванию, сетевым подключениям и аппаратным ресурсам.

- Папка scripts. Эта папка содержит скрипты и исполняемые файлы, которые используются, чтобы развернуть и настроить сетевую функцию. Например, среди скриптов могут быть задачи автоматизации, установочные операции, а также уникальные действия, выполнение которых требуется для развертывания.

В структуру пакета VNF дополнительно входит папка images, которая содержит файлы-образы, а также ресурсы, необходимые для правильного функционирования VNF, такие как двоичные файлы, прошивки и значки.

Если вам назначена роль администратора платформы, вам нужно загрузить пакет VNF и/или PNF в веб-интерфейс оркестратора, чтобы получить возможность добавлять их в топологию сетевых сервисов и применять к проходящему через эти сервисы трафику.

> Обратите внимание, что контроллер SD-WAN также разворачивается в виде VNF или PNF.

Чтобы загрузить пакет VNF или PNF в оркестратор:

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

   Отобразится страница управления сетевыми сервисами.

2. Вверху страницы нажмите на кнопку **+ VNF** или **+ PNF**.

3. Выберите файл пакета VNF или PNF.

   Загруженная сетевая функция отобразится в панели **Каталог**.

Шаблон сетевого сервиса

Вы можете создать шаблон сетевого сервиса, после чего назначить его тенантам, в рамках которых требуется развернуть этот сетевой сервис. Это позволяет вам избежать необходимости в индивидуальном создании сетевого сервиса в рамках каждого существующего тенанта.

При создании шаблона строится топология сетевого сервиса, со всеми требуемыми сетевыми компонентами, соединениями, интерфейсами, которые подключаются друг к другу. Тенант, которому назначен шаблон, может заменить абстрактные компоненты топологии на реальные и развернуть сетевой сервис.

Создание шаблона сетевого сервиса

Перед созданием шаблона требуется загрузить все необходимые пакеты VNF или PNF в оркестратор.

Чтобы создать шаблон сетевого сервиса:

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

   Отобразится страница управления сетевыми сервисами.

2. Вверху страницы нажмите на кнопку **+ Шаблон**.

   Отобразится графический конструктор для построения топологии сетевого сервиса.

3. Перетащите следующие сетевые компоненты с панели **Каталог** в графический конструктор, чтобы добавить их в топологию:

   - Виртуальные сетевые функции.
   - Физические сетевые функции.
   - Общие сетевые сервисы. Если в топологию нескольких сетевых сервисов добавлен общий сетевой сервис, его можно использовать, чтобы связать эти сетевые сервисы.
   - Шаблон сетевого сервиса. Если при создании шаблона сетевого сервиса вы помещаете в топологию другой шаблон, топология выстраивается в соответствии с помещенным шаблоном, после чего вы можете изменить ее, добавив новые компоненты или удалив существующие.

   Вы можете нажать на добавленный сетевой компонент и удалить его, выбрав в раскрывающемся списке **Удалить**.

4. Перетащите следующие соединения со вкладки **Соединения** внизу в графический конструктор, чтобы добавить их в топологию:

   - **P2P** – транспортный сервис P2P.
   - **P2M** – транспортный сервис P2M.
   - **M2M** – транспортный сервис M2M.

   Остальные соединения относятся к сетевому взаимодействию на уровне VIM и устанавливаются между VNF, хостом которых является облачная платформа OpenStack:

   - **OS shared** – сеть, которую могут делить несколько тенантов.
   - **OS vRouter** – маршрутизатор, который обеспечивает L3-маршрутизацию.
   - **OS VLAN** – сеть для передачи тегированного L2-трафика стандарта 802.1Q.
   - **OS VXLAN** – сеть для обеспечения VXLAN-туннелирования.

- **OS flat** – сеть для передачи нетегированного L2-трафика.

Вы можете нажать на добавленное соединение и удалить его, выбрав в раскрывающемся списке **Удалить**.

5. Внизу выберите вкладку **UNI** и перетащите в графический конструктор UNI и/или WAN-интерфейсы, чтобы добавить их в топологию. Вы можете нажать на добавленный интерфейс и удалить его, выбрав в раскрывающемся списке **Удалить**.

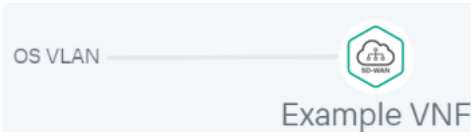
6. Настройте компоненты топологии.

7. Подключите соединения к сетевым компонентам:

   a. Нажмите на соединение и в раскрывающемся списке выберите **Добавить leaf**, чтобы подключить сетевой компонент с ролью Leaf. Если вы нажали на P2M-сервис, вы можете выбрать в раскрывающемся списке **Добавить root**, чтобы подключить сетевой компонент с ролью Root.

   b. Нажмите на значок сетевого компонента и в отобразившемся окне выберите интерфейс для подключения.

   Соединение будет подключено к сетевому компоненту, и в топологии между ними отобразится линия. Например, на рисунке ниже показана VLAN-сеть, подключенная к VNF.



8. Подключите соединения к интерфейсам:

   a. Нажмите на соединение и в раскрывающемся списке выберите **Добавить leaf**, чтобы подключить интерфейс с ролью Leaf. Если вы нажали на P2M-сервис, вы можете выбрать в раскрывающемся списке **Добавить root**, чтобы подключить интерфейс с ролью Root.

   b. Нажмите на значок интерфейса.

   Соединение будет подключено к интерфейсу, и в топологии между ними отобразится линия. Например, на рисунке ниже показан P2P-сервис, подключенный к UNI и WAN-интерфейсу.

9. При необходимости назначьте резервные интерфейсы для UNI:

   a. Нажмите на UNI и в раскрывающемся списке выберите **Зарезервировать**.

   > Резервный интерфейс можно назначить только для UNI, к которым подключено хотя бы одно соединение.

   b. Нажмите на значок интерфейса, который требуется использовать в качестве резервного.

   Интерфейс будет назначен резервным для UNI, и в топологии между UNI, резервным интерфейсом и подключенным к UNI соединением отобразится пунктирная линия. Например, на рисунке ниже WAN-интерфейс является резервным для UNI.

10. При необходимости выполните следующие действия:

    - Установите флажок **Описание**, чтобы отобразить описание под каждым компонентом топологии. По умолчанию флажок установлен.
    - Нажмите на кнопку **Выровнять**, чтобы выровнять компоненты топологии по вертикали.

11. В поле **Имя** введите имя шаблона сетевого сервиса.
12. Вверху страницы нажмите на кнопку **Сохранить**.

    Шаблон сетевого сервиса будет создан и отобразится в панели **Каталог** на вкладке **Шаблоны**.

Удаление шаблона сетевого сервиса

Удаленные шаблоны сетевых сервисов невозможно восстановить.

Чтобы удалить шаблон сетевого сервиса:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Каталог** выберите вкладку **Шаблоны**.

   Отобразится список шаблонов сетевых сервисов.

3. Нажмите на кнопку удаления ✕ рядом с шаблоном сетевого сервиса.
4. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Шаблон сетевого сервиса будет удален и перестанет отображаться в панели **Каталог**.

Создание сетевого сервиса

Вы можете создать сетевой сервис вручную или используя шаблон. Когда вы используйте шаблон при создании сетевого сервиса, топология сервиса выстраивается в соответствии с топологией шаблона, после чего вы можете изменить ее, добавив новые компоненты или удалив существующие.

Чтобы создать сетевой сервис:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на кнопку **+ Сетевой сервис**.

   Отобразится графический конструктор для построения топологии сетевого сервиса.

3. Если для создания сетевого сервиса требуется использовать шаблон, перетащите этот шаблон с панели **Каталог** в графический конструктор.

   Топология выстроится в соответствии с помещенным шаблоном.

4. Перетащите следующие сетевые компоненты с панели **Каталог** в графический конструктор, чтобы добавить их в топологию:

   - Виртуальные сетевые функции.
   - Физические сетевые функции.
   - Общие сетевые сервисы. Если в топологию нескольких сетевых сервисов добавлен общий сетевой сервис, его можно использовать, чтобы связать эти сетевые сервисы.

   При добавлении сетевой функции в открывшемся окне выберите, где ее требуется разместить – в центре обработки данных или на устройстве uCPE.

   Вы можете нажать на добавленный сетевой компонент и удалить его, выбрав в раскрывающемся списке **Удалить**.

5. Перетащите следующие соединения со вкладки **Соединения** внизу в графический конструктор, чтобы добавить их в топологию:

   - **P2P** – транспортный сервис P2P.
   - **P2M** – транспортный сервис P2M.
   - **M2M** – транспортный сервис M2M.

   Остальные соединения относятся к сетевому взаимодействию на уровне VIM и устанавливаются между VNF, хостом которых является облачная платформа OpenStack:

   - **OS shared** – сеть, которую могут делить несколько тенантов.
   - **OS vRouter** – маршрутизатор, который обеспечивает L3-маршрутизацию.
   - **OS VLAN** – сеть для передачи тегированного L2-трафика стандарта 802.1Q.
   - **OS VXLAN** – сеть для обеспечения VXLAN-туннелирования.
   - **OS flat** – сеть для передачи нетегированного L2-трафика.

   При добавлении соединения **OS VLAN**, **OS VXLAN** или **OS flat** в открывшемся окне выберите, где его требуется разместить – в центре обработки данных или на устройстве uCPE.

   Вы можете нажать на добавленное соединение и удалить его, выбрав в раскрывающемся списке **Удалить**.

6. Внизу выберите вкладку **UNI** и перетащите в графический конструктор UNI и/или WAN-интерфейсы, чтобы добавить их в топологию. Вы можете нажать на добавленный интерфейс и удалить его, выбрав в раскрывающемся списке **Удалить**.

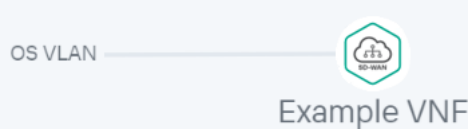
7. Настройте компоненты топологии.

8. Подключите соединения к сетевым компонентам:

a. Нажмите на соединение и в раскрывающемся списке выберите **Добавить leaf**, чтобы подключить сетевой компонент с ролью Leaf. Если вы нажали на P2M-сервис, вы можете выбрать в раскрывающемся списке **Добавить root**, чтобы подключить сетевой компонент с ролью Root.

b. Нажмите на значок сетевого компонента и в отобразившемся окне выберите интерфейс для подключения.

Соединение будет подключено к сетевому компоненту, и в топологии между ними отобразится линия. Например, на рисунке ниже показана VLAN-сеть, подключенная к VNF.

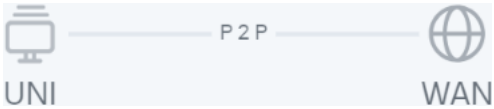


9. Подключите соединения к интерфейсам:

a. Нажмите на соединение и в раскрывающемся списке выберите **Добавить leaf**, чтобы подключить интерфейс с ролью Leaf. Если вы нажали на P2M-сервис, вы можете выбрать в раскрывающемся списке **Добавить root**, чтобы подключить интерфейс с ролью Root.

b. Нажмите на значок интерфейса.

Соединение будет подключено к интерфейсу, и в топологии между ними отобразится линия. Например, на рисунке ниже показан P2P-сервис, подключенный к UNI и WAN-интерфейсу.



10. При необходимости назначьте резервные интерфейсы для UNI:

a. Нажмите на UNI и в раскрывающемся списке выберите **Зарезервировать**.

> Резервный интерфейс можно назначить только для UNI, к которым подключено хотя бы одно соединение.

b. Нажмите на значок интерфейса, который требуется использовать в качестве резервного.

Интерфейс будет назначен резервным для UNI, и в топологии между UNI, резервным интерфейсом и подключенным к UNI соединением отобразится пунктирная линия. Например, на рисунке ниже WAN-интерфейс является резервным для UNI.

11. При необходимости выполните следующие действия:

- Установите флажок **Описание**, чтобы отобразить описание под каждым компонентом топологии. По умолчанию флажок установлен.

- Нажмите на кнопку **Выровнять**, чтобы выровнять компоненты топологии по вертикали.

12. В поле **Имя** введите имя сетевого сервиса.

13. Завершите создание сетевого сервиса:

    - Если вы хотите сохранить сетевой сервис, нажмите на кнопку **Сохранить**.

    - Если вы хотите сохранить и сразу 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**.

Настройка компонентов топологии сетевого сервиса

Вы можете настроить сетевые компоненты, соединения и интерфейсы, добавленные в топологию шаблона сетевого сервиса или отдельного сетевого сервиса. Перед настройкой компонентов топологии ее необходимо открыть.

Чтобы открыть топологию:

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

   Отобразится страница управления сетевыми сервисами.

2. Откройте топологию:

   - Если вы хотите открыть топологию шаблона сетевого сервиса, в панели **Каталог** выберите шаблон.

   - Если вы хотите открыть топологию сетевого сервиса, в панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

Для настройки компонентов топологии используйте следующие инструкции:

- Настройка VNF в топологии шаблона сетевого сервиса.

Чтобы настроить VNF в топологии:

1. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

2. Выберите вкладку **Точки подключения** и настройте интерфейсы VNF:

   a. В раскрывающемся списке **Тип** выберите, каким образом требуется назначить интерфейсу IP-адрес и маску подсети:

      - **DHCP reservation** – назначить IP-адрес и маску подсети с помощью DHCP.
      - **AUTO** – автоматически назначить IP-адрес и маску подсети. Это значение выбрано по умолчанию.

   b. Если в раскрывающемся списке **Тип** вы выбрали **DHCP reservation**, выполните следующие действия:

      1. В поле **IP** введите IP-адрес интерфейса.
      2. В поле **Маска** введите маску подсети.

   c. В поле **Описание** введите краткое описание интерфейса.

   d. При необходимости сделать интерфейс магистральным портом (англ. trunk port) и обрабатывать трафик нескольких VLAN одновременно установите флажок **Магистраль**. Когда флажок установлен, интерфейс VNF способен передавать и получать тегированный VLAN-трафик, который содержит дополнительный идентификатор (VLAN-тег), позволяющий определять и фильтровать разные VLAN в сети. По умолчанию флажок снят.

3. Выберите вкладку **Параметры VNF** и укажите общие параметры VNF:

   a. В поле **Имя** введите имя VNF.

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

   c. В поле **Порядок** введите порядковый номер для развертывания VNF в облачной платформе OpenStack. Когда вы развертываете сетевой сервис, VNF с наименьшим значением порядкового номера развертывается первой. Если в параметрах ни одной из добавленных в топологию сетевого сервиса VNF не указан порядковый номер, все VNF развертываются одновременно.

4. Укажите требуемые параметры на оставшихся вкладках. Количество вкладок, на которых вы можете настроить параметры, зависит от содержания пакета VNF. Вкладки добавляются в пакет как переменные.

   Если у вас возникают трудности с настройкой определенных параметров, мы рекомендуем обратиться к технической документации поставщика VNF или в техническую поддержку "Лаборатории Касперского".

5. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка PNF в топологии шаблона сетевого сервиса.

Чтобы настроить PNF в топологии:

1. Нажмите на PNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете PNF.

2. Выберите вкладку **Параметры PNF** и укажите общие параметры PNF:

   a. В поле **Имя** введите имя PNF.

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

   c. В поле **Порядок** введите порядковый номер для развертывания PNF. Когда вы развертываете сетевой сервис, PNF с наименьшим значением порядкового номера развертывается первой. Если в параметрах ни одной из добавленных в топологию сетевого сервиса PNF не указан порядковый номер, все PNF развертываются одновременно.

3. Выберите вкладку **Размещение в ЦОД** и выберите, в каком центре обработки данных размещена PNF:

   a. В поле **Центр обработки данных** введите имя центра обработки данных и в раскрывающемся списке выберите требуемое значение.

   b. Нажмите на кнопку **Применить**.

4. Выберите вкладку **Management IP** и в полях **IP** введите IP-адреса управляющих интерфейсов VDU в составе PNF. Вы можете проверить доступность адреса, нажав на кнопку **Проверить соединение**.

5. Укажите требуемые параметры на оставшихся вкладках. Количество вкладок, на которых вы можете настроить параметры, зависит от содержания пакета PNF. Вкладки добавляются в пакет как переменные.

   Если у вас возникают трудности с настройкой определенных параметров, мы рекомендуем обратиться к технической документации поставщика PNF или в техническую поддержку "Лаборатории Касперского".

6. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка P2P-сервиса в топологии шаблона сетевого сервиса.

Чтобы настроить P2P-сервис в топологии:

1. Нажмите на P2P-сервис.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

2. В поле **Имя** введите имя транспортного сервиса.

3. При необходимости в поле **Описание** введите краткое описание транспортного сервиса.

4. Вверху области настройки нажмите на кнопку **Сохранить**.

- **Настройка P2M-сервиса в топологии шаблона сетевого сервиса**.

Чтобы настроить P2M-сервис в топологии:

1. Нажмите на P2M-сервис.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

2. В поле **Имя** введите имя транспортного сервиса.

3. При необходимости в поле **Описание** введите краткое описание транспортного сервиса.

4. В поле **Точки подключения** введите максимальное количество точек подключения (англ. connection points) к транспортному сервису. Диапазон значений: от 2 до 9999. Если вы не указываете значение для этого параметра, количество точек подключения не ограничивается.

5. В раскрывающемся списке **Режим** выберите, требуется ли использовать Default Forwarding Interface (далее DFI) в транспортном сервисе. Если сервисному интерфейсу назначена роль DFI, на него отправляется весь неизвестный unicast-трафик (англ. unknown unicast). Доступные значения:

   - **Классический** – не использовать DFI. Это значение выбрано 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.

6. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 10 до 65 535. По умолчанию указано значение `300`.

7. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое требуется применить к серии кадров, когда первый кадр отправляется на контроллер SD-WAN 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 сервисные интерфейсы, добавленные в транспортный сервис, за исключением интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.
   - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отбрасывается.

   В обоих случаях при наличии MAC-адреса назначения в таблице MAC-адресов серия кадров отправляется на соответствующий сервисный интерфейс.

8. В поле **Размер MAC-таблицы** введите максимальное количество записей в MAC-таблице на контроллере SD-WAN. 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 на контроллере SD-WAN:

   - **Flood** – трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.

   - **Drop** – трафик с ранее неизученными MAC-адресами назначения не передается.

10. При необходимости используйте OpenStack DHCP, чтобы автоматически назначить IP-адреса и параметры конфигурации виртуальным машинам:

    a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**.

    b. В поле **CIDR** введите IP-адрес и маску подсети OpenStack.

    c. В поле **Шлюз** введите IP-адрес шлюза для маршрутизации трафика, покидающего виртуальную сеть. Шлюз соединяет виртуальную сеть с внешними сетями, например с интернетом. Адрес шлюза должен находится в одной подсети с виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом.

    d. При необходимости создать диапазон IP-адресов в блоке **Пулы** нажмите на кнопку **+ Пул** и в отобразившихся полях введите начальное и конечное значение диапазона. Если виртуальная машина запрашивает IP-адрес, DHCP-сервер назначает ей адрес из диапазона.

    Диапазон должен находится в одной подсети со шлюзом, виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом, а его размер должен соответствовать количеству виртуальных машин в сети. Вы можете создать несколько диапазонов и удалить диапазон, нажав на кнопку **Удалить** рядом с ним.

    e. При необходимости добавить DNS-сервер в блоке **DNS** нажмите на кнопку **DNS** и в отобразившемся поле введите IP-адрес сервера. DNS-сервер позволяет виртуальным машинам преобразовывать доменные имена в IP-адреса.

    Информация с DNS-сервера передается виртуальным машинам посредством DHCP-опций, после чего они могут взаимодействовать с устройствами внутри виртуальной сети, а также получать доступ в интернет и другие внешние сети, используя доменные имена вместо IP-адресов. Вы можете добавить несколько серверов и удалить сервер, нажав на кнопку **Удалить** рядом с ним.

11. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка M2M-сервиса в топологии шаблона сетевого сервиса.

Чтобы настроить M2M-сервис в топологии:

1. Нажмите на M2M-сервис.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

2. В поле **Имя** введите имя транспортного сервиса.

3. При необходимости в поле **Описание** введите краткое описание транспортного сервиса.

4. В поле **Точки подключения** введите максимальное количество точек подключения (англ. connection points) к транспортному сервису. Диапазон значений: от 2 до 9999. Если вы не указываете значение для этого параметра, количество точек подключения не ограничивается.

5. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 10 до 65 535. По умолчанию указано значение `300`.

6. В раскрывающемся списке **Режим изучения MAC** выберите действие, которое требуется применить к серии кадров, когда первый кадр отправляется на контроллер SD-WAN 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 сервисные интерфейсы, добавленные в транспортный сервис, за исключением интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.

   - **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отбрасывается.

   В обоих случаях при наличии MAC-адреса назначения в таблице MAC-адресов серия кадров отправляется на соответствующий сервисный интерфейс.

7. В поле **Размер MAC-таблицы** введите максимальное количество записей в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 0 до 65 535. Вы можете ввести `0`, чтобы не ограничивать количество записей. По умолчанию указано значение `100`.

8. В раскрывающемся списке **Перегрузка MAC-таблицы** выберите политику обработки новых MAC-адресов при переполнении MAC-таблицы на контроллере SD-WAN:

   - **Flood** – трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано по умолчанию.

   - **Drop** – трафик с ранее неизученными MAC-адресами назначения не передается.

9. При необходимости используйте OpenStack DHCP, чтобы автоматически назначить IP-адреса и параметры конфигурации виртуальным машинам:

   a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**.

   b. В поле **CIDR** введите IP-адрес и маску подсети OpenStack.

c. В поле **Шлюз** введите IP-адрес шлюза для маршрутизации трафика, покидающего виртуальную сеть. Шлюз соединяет виртуальную сеть с внешними сетями, например с интернетом. Адрес шлюза должен находится в одной подсети с виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом.

d. При необходимости создать диапазон IP-адресов в блоке **Пулы** нажмите на кнопку **+ Пул** и в отобразившихся полях введите начальное и конечное значение диапазона. Если виртуальная машина запрашивает IP-адрес, DHCP-сервер назначает ей адрес из диапазона.

   Диапазон должен находится в одной подсети со шлюзом, виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом, а его размер должен соответствовать количеству виртуальных машин в сети. Вы можете создать несколько диапазонов и удалить диапазон, нажав на кнопку **Удалить** рядом с ним.

e. При необходимости добавить DNS-сервер в блоке **DNS** нажмите на кнопку **DNS** и в отобразившемся поле введите IP-адрес сервера. DNS-сервер позволяет виртуальным машинам преобразовывать доменные имена в IP-адреса.

   Информация с DNS-сервера передается виртуальным машинам посредством DHCP-опций, после чего они могут взаимодействовать с устройствами внутри виртуальной сети, а также получать доступ в интернет и другие внешние сети, используя доменные имена вместо IP-адресов. Вы можете добавить несколько серверов и удалить сервер, нажав на кнопку **Удалить** рядом с ним.

- При необходимости разрешить совместное использование M2M-сервиса разными сетевыми сервисами установите флажок **Поделиться сетевым сервисом**. По умолчанию флажок снят.

10. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка общей сети (OS 2 SHARED) в топологии шаблона сетевого сервиса.

Чтобы настроить общую сеть в топологии:

1. Нажмите на общую сеть.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

2. В поле **Имя** введите имя общей сети.

3. При необходимости в поле **Описание** введите краткое описание общей сети.

4. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка виртуального маршрутизатора (OS vRouter) в топологии шаблона сетевого сервиса.

Чтобы настроить виртуальный маршрутизатор в топологии:

1. Нажмите на виртуальный маршрутизатор.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

2. В поле **Имя** введите имя виртуального маршрутизатора.

3. При необходимости в поле **Описание** введите краткое описание виртуального маршрутизатора.

4. При необходимости выставить значение up для рабочего состояния виртуального маршрутизатора установите флажок **Административное состояние**. Этот флажок позволяет вам управлять рабочим состоянием маршрутизатора без необходимости в его повторном удалении/создании. Когда флажок установлен, маршрутизатор может передавать трафик. По умолчанию флажок снят.

5. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка VLAN в топологии шаблона сетевого сервиса.

Чтобы настроить VLAN в топологии:

1. Нажмите на VLAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

2. В поле **Имя** введите имя VLAN.

3. При необходимости в поле **Описание** введите краткое описание VLAN.

4. При необходимости используйте OpenStack DHCP, чтобы автоматически назначить IP-адреса и параметры конфигурации виртуальным машинам:

   a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**.

   b. В поле **CIDR** введите IP-адрес и маску подсети OpenStack.

   c. В поле **Шлюз** введите IP-адрес шлюза для маршрутизации трафика, покидающего виртуальную сеть. Шлюз соединяет виртуальную сеть с внешними сетями, например с интернетом. Адрес шлюза должен находится в одной подсети с виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом.

   d. При необходимости создать диапазон IP-адресов в блоке **Пулы** нажмите на кнопку **+ Пул** и в отобразившихся полях введите начальное и конечное значение диапазона. Если виртуальная машина запрашивает IP-адрес, DHCP-сервер назначает ей адрес из диапазона.

      Диапазон должен находится в одной подсети со шлюзом, виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом, а его размер должен соответствовать количеству виртуальных машин в сети. Вы можете создать несколько диапазонов и удалить диапазон, нажав на кнопку **Удалить** рядом с ним.

   e. При необходимости добавить DNS-сервер в блоке **DNS** нажмите на кнопку **DNS** и в отобразившемся поле введите IP-адрес сервера. DNS-сервер позволяет виртуальным машинам преобразовывать доменные имена в IP-адреса.

      Информация с DNS-сервера передается виртуальным машинам посредством DHCP-опций, после чего они могут взаимодействовать с устройствами внутри виртуальной сети, а также получать доступ в интернет и другие внешние сети, используя доменные имена вместо IP-адресов. Вы можете добавить несколько серверов и удалить сервер, нажав на кнопку **Удалить** рядом с ним.

5. При необходимости разрешить совместное использование сети разными сетевыми сервисами установите флажок **Поделиться сетью**. По умолчанию флажок снят.

6. При необходимости сегментировать сеть на несколько VLAN в поле **ID сегментации** введите VLAN ID.

7. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка VXLAN в топологии шаблона сетевого сервиса.

Чтобы настроить VXLAN в топологии:

1. Нажмите на VXLAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

2. В поле **Имя** введите имя VXLAN-сети.

3. При необходимости в поле **Описание** введите краткое описание VXLAN-сети.

4. При необходимости используйте OpenStack DHCP, чтобы автоматически назначить IP-адреса и параметры конфигурации виртуальным машинам:

   a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**.

   b. В поле **CIDR** введите IP-адрес и маску подсети OpenStack.

   c. В поле **Шлюз** введите IP-адрес шлюза для маршрутизации трафика, покидающего виртуальную сеть. Шлюз соединяет виртуальную сеть с внешними сетями, например с интернетом. Адрес шлюза должен находится в одной подсети с виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом.

   d. При необходимости создать диапазон IP-адресов в блоке **Пулы** нажмите на кнопку **+ Пул** и в отобразившихся полях введите начальное и конечное значение диапазона. Если виртуальная машина запрашивает IP-адрес, DHCP-сервер назначает ей адрес из диапазона.

      Диапазон должен находится в одной подсети со шлюзом, виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом, а его размер должен соответствовать количеству виртуальных машин в сети. Вы можете создать несколько диапазонов и удалить диапазон, нажав на кнопку **Удалить** рядом с ним.

   e. При необходимости добавить DNS-сервер в блоке **DNS** нажмите на кнопку **DNS** и в отобразившемся поле введите IP-адрес сервера. DNS-сервер позволяет виртуальным машинам преобразовывать доменные имена в IP-адреса.

      Информация с DNS-сервера передается виртуальным машинам посредством DHCP-опций, после чего они могут взаимодействовать с устройствами внутри виртуальной сети, а также получать доступ в интернет и другие внешние сети, используя доменные имена вместо IP-адресов. Вы можете добавить несколько серверов и удалить сервер, нажав на кнопку **Удалить** рядом с ним.

5. При необходимости разрешить совместное использование сети разными сетевыми сервисами установите флажок **Поделиться сетью**. По умолчанию флажок снят.

6. При необходимости сегментировать сеть на несколько VXLAN в поле **ID сегментации** введите VXLAN ID.

7. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка плоской сети в топологии шаблона сетевого сервиса.

Чтобы настроить плоскую сеть в топологии:

1. Нажмите на плоскую сеть.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

2. В поле **Имя** введите имя плоской сети.

3. При необходимости в поле **Описание** введите краткое описание плоской сети.

4. При необходимости используйте OpenStack DHCP, чтобы автоматически назначить IP-адреса и параметры конфигурации виртуальным машинам:

   a. В раскрывающемся списке **OpenStack DHCP** выберите **Включено**.

   b. В поле **CIDR** введите IP-адрес и маску подсети OpenStack.

   c. В поле **Шлюз** введите IP-адрес шлюза для маршрутизации трафика, покидающего виртуальную сеть. Шлюз соединяет виртуальную сеть с внешними сетями, например с интернетом. Адрес шлюза должен находится в одной подсети с виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом.

   d. При необходимости создать диапазон IP-адресов в блоке **Пулы** нажмите на кнопку **+ Пул** и в отобразившихся полях введите начальное и конечное значение диапазона. Если виртуальная машина запрашивает IP-адрес, DHCP-сервер назначает ей адрес из диапазона.

      Диапазон должен находится в одной подсети со шлюзом, виртуальными машинами и другими сетевыми устройствами, чтобы они могли взаимодействовать друг с другом, а его размер должен соответствовать количеству виртуальных машин в сети. Вы можете создать несколько диапазонов и удалить диапазон, нажав на кнопку **Удалить** рядом с ним.

   e. При необходимости добавить DNS-сервер в блоке **DNS** нажмите на кнопку **DNS** и в отобразившемся поле введите IP-адрес сервера. DNS-сервер позволяет виртуальным машинам преобразовывать доменные имена в IP-адреса.

      Информация с DNS-сервера передается виртуальным машинам посредством DHCP-опций, после чего они могут взаимодействовать с устройствами внутри виртуальной сети, а также получать доступ в интернет и другие внешние сети, используя доменные имена вместо IP-адресов. Вы можете добавить несколько серверов и удалить сервер, нажав на кнопку **Удалить** рядом с ним.

5. При необходимости разрешить совместное использование сети разными сетевыми сервисами установите флажок **Поделиться сетью**. По умолчанию флажок снят.

6. Вверху области настройки нажмите на кнопку **Сохранить**.

- Настройка интерфейсов в топологии шаблона сетевого сервиса

Чтобы настроить интерфейс в топологии:

1. Нажмите на интерфейс.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

2. В поле **Имя** введите имя интерфейса.

3. При необходимости в поле **Описание** введите краткое описание интерфейса.

4. Вверху области настройки нажмите на кнопку **Сохранить**.

Изменение топологии сетевого сервиса

Чтобы изменить топологию сетевого сервиса:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Вверху страницы нажмите на кнопку **Изменить**.

4. Внесите требуемые изменения в топологию сетевого сервиса. Описание параметров см. в следующих инструкциях:

   - Инструкция по созданию сетевого сервиса.
   - Инструкция по настройке компонентов топологии сетевого сервиса.

5. Нажмите на кнопку **Развернуть изменения**.

Развертывание сетевого сервиса

Если во время развертывания сетевого сервиса отсутствует связь между оркестратором и uCPE, развертывание 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.

   Топология сетевого сервиса отобразится в графическом конструкторе.

3. Вверху страницы нажмите на кнопку **Развернуть**.

   Начнется развертывание сетевого сервиса, которое может длиться несколько минут. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

Проверка согласованности работы сетевого сервиса

Проверка на согласованность (англ. consistency check) позволяет убедиться в правильности конфигурации сетевого сервиса. В ходе проверки выявляются проблемы и конфликты в указанных параметрах, которые могут привести к неработоспособности всего 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 кнопку настройки рядом с сетевым сервисом и в раскрывающемся списке выберите **Проверить согласованность**.

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

   Начнется проверка на согласованность.

Повторное развертывание сетевого сервиса и его компонентов

Вы можете повторно развернуть сетевой сервис или его компонент, чтобы применить изменения, внесенные в конфигурацию, обновить используемое программное обеспечение до последней версии или восстановить работу в случае возникновения неполадок.

Обратите внимание, что повторное развертывание может привести к краткосрочным перебоям в 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.

Для повторного развертывания сетевого сервиса или его компонента используйте следующие инструкции:

- Повторное развертывание сетевого сервиса

Повторное развертывание также позволяет исправить проблемы с производительностью сетевого сервиса и избавиться от узких мест (англ. bottlenecks).

Чтобы повторно развернуть сетевой сервис:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** нажмите на кнопку настройки рядом с сетевым сервисом и в раскрывающемся списке выберите **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**.

- Повторное развертывание VNF.

Чтобы повторно развернуть VNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Вверху области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Повторно развернуть VNF**.

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

Начнется повторное развертывание VNF, которое может длиться несколько минут. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

- Повторное развертывание VDU.

Чтобы повторно развернуть VDU:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Повторно развернуть VDU**.

6. В открывшемся окне подтверждения нажмите на кнопку **Подтвердить**.

Начнется повторное развертывание VDU, которое может длиться несколько минут. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

Функция Auto-Healing

Функция Auto-Healing автоматически обнаруживает возникающие в ходе работы сетевого сервиса проблемы и предпринимает необходимые действия для их исправления. Среди таких действий может быть перезапуск неработающих компонентов, замена недоступных сетевых ресурсов или перенаправление трафика в сохранившие работоспособность виртуальные машины / экземпляры.

Если функция включена для сетевого сервиса, его компоненты восстанавливаются автоматически. Если функция выключена, для восстановления работы компонентов требуется ручное вмешательство со стороны администратора. По умолчанию функция включена.

При необходимости вы можете использовать Auto-Healing для отдельных компонентов сетевого сервиса, даже если функция выключена. Для использования функции Auto-Healing используйте следующие инструкции:

- Включение и выключение функции Auto-Healing для сетевого сервиса.
- Использование функции Auto-Healing для VNF.

Чтобы использовать функцию Auto-Healing для VNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Вверху области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Восстановление VNF**.

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

Начнется автоматическое восстановление VNF.

- Использование функции Auto-Healing для VDU.

Чтобы использовать функцию Auto-Healing для VDU:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Восстановление VDU**.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Начнется автоматическое восстановление VDU.

Управление VNF и VDU в сетевом сервисе

После развертывания сетевого сервиса, вы можете управлять VNF, а также VDU (Virtual Deployment Unit), входящими в их состав.

VDU – это виртуальная машина, которая является хостом VNF. Она 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.

Выбор варианта развертывания (flavour) VNF

Варианты развертывания (англ. flavours) указываются в пакете VNF и используются, чтобы определить характеристики и спецификации экземпляра VNF. Каждый вариант развертывания является предопределенным набором назначенных ресурсов, таких как ЦПУ, память и полоса пропускания. Эти ресурсы определяют возможности экземпляра VNF и влияют на его производительность.

Чтобы выбрать вариант развертывания VNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Нажмите на кнопку **Масштабировать** рядом с вариантом развертывания.

VNF будет масштабирована до выбранного варианта развертывания.

Просмотр параметров VDU

Чтобы просмотреть параметры VDU:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на имя VDU, параметры которой требуется просмотреть.

Откроется окно с параметрами VDU.

Остановка и запуск VNF и VDU

Остановка VNF/VDU позволяет выполнять их поддержку и устанавливать обновления для программного обеспечения.

Если VNF/VDU не используется, ее можно остановить, чтобы освободить вычислительные ресурсы и использовать их для выполнения других задач. Вы также можете остановить VNF/VDU, провоцирующую появление ошибок и сбоев, чтобы изолировать проблемный компонент и решить проблему, при этом сохранив работоспособность.

Для остановки VNF или VDU используйте следующие инструкции:

- Остановка VNF.

Когда вы останавливаете VNF, она перестает предоставляться в рамках сетевого сервиса. Мы рекомендуем планировать остановку VNF таким образом, чтобы она не затрагивала работу сетевого сервиса.

Чтобы остановить VNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Вверху области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Управление питанием** → **Остановить VNF**.

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

VNF будет остановлена.

- Остановка VDU.

Когда вы останавливаете VDU, она перестает предоставляться в рамках VNF. Мы рекомендуем планировать остановку VDU таким образом, чтобы она не затрагивала работу VNF.

Чтобы остановить VDU:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Управление питанием → Остановить VDU**.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

VDU будет остановлена.

При необходимости вы можете снова запустить остановленную VNF или VDU. Для этого используйте следующие инструкции:

- Запуск VNF.

Чтобы запустить VNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Вверху области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Запустить VNF**.

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

VNF будет запущена.

- Запуск VDU.

Чтобы запустить VDU:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Запустить VDU**.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

VDU будет запущена.

Временная остановка и запуск VNF и VDU

Вы можете поставить VNF/VDU на паузу или перевести в состояние ожидания, чтобы освободить системные ресурсы, например ЦПУ и память, и предоставить их другим компонентам, которые имеют более высокий приоритет. Это может потребоваться, когда происходит временное снижение пользовательской активности и необходимости в предоставлении сетевых функций. Такой подход к управлению сохраняет ресурсы и обеспечивает их наиболее эффективное использование.

Разница между VNF/VDU, поставленной на паузу и переведенной в состояние ожидания, заключается в том, что при переводе в состояние ожидания на диск VNF/VDU сохраняется информация о ее конфигурации. Это позволяет полностью выключить VNF/VDU и перенести на другую хост-машину. Когда VNF/VDU снова переводится в активное состояние, ее конфигурация полностью восстанавливается.

Для временной остановки VNF/VDU используйте следующие инструкции:

- **Пауза VNF и перевод в состояние ожидания**.

  Чтобы поставить VNF на паузу или перевести в состояние ожидания:

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

     Отобразится страница управления сетевыми сервисами.

  2. В панели **Сетевые сервисы** выберите сетевой сервис.

     Отобразится графический конструктор с топологией сетевого сервиса.

  3. Нажмите на VNF.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

     По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

  4. Вверху области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Поставить VNF на паузу** или **Приостановить VNF**.

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

  VNF будет поставлена на паузу или переведена в состояние ожидания.

- **Пауза VDU и перевод в состояние ожидания**.

Чтобы поставить VDU на паузу или перевести в состояние ожидания:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Поставить VDU на паузу** или **Приостановить VDU**.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

VDU будет поставлена на паузу или переведена в состояние ожидания.

При необходимости вы можете снять VNF/VDU с паузы или перевести обратно в активное состояние. Для этого используйте следующие инструкции:

- Снятие с паузы VNF и перевод в активное состояние.

Чтобы снять VNF с паузы или перевести в активное состояние:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Вверху области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Снять паузу с VNF** или **Возобновить приостановленную VNF**.

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

VNF будет снята с паузы или переведена в активное состояние.

- Снятие с паузы VDU и перевод в активное состояние.

Чтобы снять VDU с паузы или перевести в активное состояние:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Снять паузу с VDU** или **Возобновить приостановленную VNF**.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

VDU будет снята с паузы или переведена в активное состояние.

Программная перезагрузка VNF и VDU

Программная перезагрузка (англ. soft reboot) VNF/VDU может использоваться, чтобы без нарушения работы установить обновления для программного обеспечения, включая исправления ошибок, улучшения безопасности и новые возможности.

Вы также можете программно перезагрузить VNF/VDU, чтобы восстановить ее стабильность за счет очищения временных или поврежденных данных, которые часто являются причиной возникновения ошибок и неисправностей.

Если VNF/VDU работает на протяжении длительного периода времени, ее программная перезагрузка может оптимизировать работу, так как при перезагрузке происходит освобождение не используемых вычислительных ресурсов.

Для программной перезагрузки VNF/VDU используйте следующие инструкции:

- Программная перезагрузка VNF.

Чтобы выполнить программную перезагрузку VNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Вверху области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Программная перезагрузка VNF**.

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

Произойдет программная перезагрузка VNF.

- Программная перезагрузка VDU.

Чтобы выполнить программную перезагрузку VDU:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Программная перезагрузка VDU**.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Произойдет программная перезагрузка VDU.

Аппаратная перезагрузка VNF и VDU

Аппаратная перезагрузка (англ. hard reboot) может использоваться, чтобы восстановить нормальное функционирование VNF/VDU, если она не отвечает на запросы или происходит несколько серьезных системных ошибок. При выполнении аппаратной перезагрузки VNF/VDU проходит через цикл выключения/включения, после чего возвращается в последнее стабильное состояние.

Обратите внимание, что аппаратная перезагрузка может привести к временной недоступности VNF/VDU.

Мы рекомендуем использовать аппаратную перезагрузку, только если все остальные меры по исправлению проблем, включая программную перезагрузку, не дали требуемых результатов.

Для аппаратной перезагрузки VNF/VDU используйте следующие инструкции:

- Аппаратная перезагрузка VNF.

  Чтобы выполнить аппаратную перезагрузку VNF:

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

     Отобразится страница управления сетевыми сервисами.

  2. В панели **Сетевые сервисы** выберите сетевой сервис.

     Отобразится графический конструктор с топологией сетевого сервиса.

  3. Нажмите на VNF.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

     По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

  4. Вверху области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Аппаратная перезагрузка VNF**.

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

  Произойдет аппаратная перезагрузка VNF.

- Аппаратная перезагрузка VDU.

Чтобы выполнить аппаратную перезагрузку VDU:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Аппаратная перезагрузка VDU**.

6. В открывшемся окне подтверждения нажмите на кнопку **Применить**.

Произойдет аппаратная перезагрузка VDU.

Мгновенный снимок состояния VDU

Мгновенный снимок (англ. snapshot) состояния VDU содержит ее полную конфигурацию и может быть использован для восстановления этой VDU при возникновении неполадок.

Вы можете сделать мгновенные снимки разных версий VDU, что особенно актуально на ранних стадиях развертывания и тестирования. Если внесенное обновление или модификация приводит к появлению проблем, вы можете вернуться к последней стабильной версии, используя соответствующий мгновенный снимок. Таким образом, мгновенные снимки позволяют изолировать ошибки и осуществлять контроль версий.

При необходимости выполнить масштабирование VDU, развернув несколько идентичных экземпляров, вы также можете использовать мгновенные снимки.

Чтобы сделать мгновенный снимок состояния VDU:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Управление VDU**.

   Отобразится таблица VDU.

5. Нажмите на кнопку **Управление** рядом с VDU и в раскрывающемся списке выберите **Снимок**.

   Откроется окно, в котором отображается таблица мгновенных снимков.

6. В поле **Имя** введите имя мгновенного снимка.

7. В поле **Описание** введите краткое описание мгновенного снимка.

8. Нажмите на кнопку **Создать**.

Мгновенный снимок будет создан и отобразится в таблице.

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 кнопку настройки рядом с сетевым сервисом и в раскрывающемся списке выберите **Открыть журнал**.

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 кнопку настройки рядом с сетевым сервисом и в раскрывающемся списке выберите **Удалить**.

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

Сетевой сервис будет удален и перестанет отображаться в панели **Сетевые сервисы**.

Управление запросами на подтверждение

Запросы на подтверждение автоматически создаются в веб-интерфейсе оркестратора, когда пользователь с недостаточными правами выполняет операции с компонентами решения. Вы определяете, требуется ли для выполнения операций пользователя подтверждение администратора при создании этого пользователя.

Созданный запрос можно подтвердить, отклонить или удалить. При подтверждении запроса происходит выполнение связанной с ним операции. Отклоненные запросы сохраняются в веб-интерфейсе.

Администраторы могут просматривать запросы на подтверждение, чтобы оценить возможные последствия выполнения операций, что предотвращает выполнение запрещенных или случайных операций с критически важными для работы Kaspersky SD-WAN компонентами. Запросы на подтверждение также можно использовать при проведении внутренних аудитов, чтобы просматривать операции, выполненные пользователями, и администраторов, подтвердивших или отклонивших выполнение этих операций.

Просмотр запросов на подтверждение

Чтобы просмотреть запросы на подтверждение,

в меню перейдите в раздел **Подтверждение**.

Отобразится таблица запросов на подтверждение. По умолчанию отображаются запросы за весь период и с любым статусом. Вы можете отобразить только нужные вам запросы с помощью фильтров вверху страницы.

Подтверждение, отклонение и удаление запросов на подтверждение

Чтобы подтвердить, отклонить или удалить запрос на подтверждение:

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

   Отобразится таблица запросов на подтверждение.

2. Выполните требуемое действие с запросом на подтверждение:

   - Нажмите на кнопку **Разрешить**, чтобы подтвердить запрос.
   - Нажмите на кнопку **Отклонить**, чтобы отклонить запрос.
   - Нажмите на кнопку **Удалить**, чтобы удалить запрос.

Управление пользователями

Пользователям необходимо аутентифицироваться в веб-интерфейсе оркестатора, чтобы работать с Kaspersky SD-WAN. Вы можете создать пользователей, учетные данные которых хранятся в локальной базе данных решения или на удаленном LDAP-сервере. Если вы планируете использовать LDAP-аутентификацию, вам нужно предварительно настроить подключение оркестратора к LDAP-серверу.

Решение поддерживает импорт групп пользователей из внешних LDAP-серверов. В этом случае требуется создать группу пользователей, соответствующую группе на удаленном сервере, после чего пользователи могут аутентифицироваться, используя имя группы.

При создании как отдельных пользователей, так и групп им можно назначить права доступа, определяющие доступ к разделам и/или подразделам веб-интерфейса.

Создание LDAP-подключения

Вам нужно создать LDAP-подключение, чтобы ваши пользователи могли аутентифицироваться в веб-интерфейсе оркестратора, используя учетные данные, хранящиеся на удаленном LDAP-сервере. Поддерживаются следующие LDAP-серверы:

- OpenLDAP с Simple-аутентификацией и Simple SSL-аутентификацией.
- Microsoft Active Directory с Kerberos-аутентификацией и Kerberos SSL-аутентификацией.

Оркестратор не может вносить изменения на подключенном LDAP-сервере.

Чтобы настроить подключение оркестратора к удаленному LDAP-серверу:

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

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

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

   Отобразится таблица LDAP-подключений.

3. Вверху страницы нажмите на кнопку **+ LDAP**.

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

5. В поле **Домен** введите FQDN домена, в котором находится LDAP-сервер.

6. В поле **Альтернативное имя домена** введите альтернативное имя домена (как правило, NETBIOS-имя). Альтернативное имя используется при создании и аутентификации пользователей наряду с FQDN домена. Например, если FQDN домена – example.com, а альтернативное имя – example, пользователи могут ввести следующие значения при аутентификации:

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

- `example\admin`.

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

   - ldap://<имя хоста>:<номер порта> – для стандартного LDAP-сервера. Порт по умолчанию: 389.

   - ldaps://<имя хоста>:<номер порта> – для LDAP-сервера с SSL-аутентификацией. Порт по умолчанию: 636.

   Например, если вы вводите `ldap://example.com:100`, имя хоста LDAP-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 LDAP-сервера. Поддерживаются следующие форматы базового различающегося имени:

   - OU=<значение>,OU=<значение> – для аутентификации в OpenLDAP. Базовое различающееся имя состоит из одного или нескольких атрибутов OU, обозначающих структуру организационных единиц (англ. organizational units) в директории LDAP-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.

   - DC=<значение>,DC=<значение> – для аутентификации в Microsoft Active Directory. Базовое различающееся имя состоит из двух атрибутов DC, обозначающих компоненты домена (англ. domain components) LDAP-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 LDAP-сервера:

   - **uid (OpenLDAP)** – идентификатор пользователя uid (user ID) для поиска в OpenLDAP. Это значение выбрано по умолчанию.

   - **sAMAccountName (Active Directory)** – пре-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 LDAP-сервере. Поддерживаются следующие форматы различающегося имени:

    - UID=<значение>,OU=<значение> – для аутентификации в OpenLDAP. Различающееся имя состоит из одного атрибута UID и одного или нескольких атрибутов OU. Атрибут UID обозначает идентификатор пользователя, в то время как атрибуты OU обозначают структуру организационных единиц в директории LDAP-сервера, в которой находится этот пользователь. Например, если вы вводите `UID=user_example,OU=OU_example`, для аутентификации оркестратора в LDAP-сервере используется пользователь с идентификатором user_example, который находится в организационной единице OU_example.

    - CN=<значение>,OU=<значение>,DC=<значение>,DC=<значение> – для аутентификации в Microsoft Active Directory. Различающееся имя состоит из одного атрибута CN, одного или нескольких атрибутов OU, а также двух атрибутов DC. Атрибут CN обозначает общее имя (англ. common name) пользователя, в то время как атрибуты OU обозначают структуру организационных единиц в директории LDAP-сервера, в которой находится этот пользователь. Последние два атрибута DC обозначают компоненты домена, в котором находится пользователь. Например, если вы вводите `CN=user_example,OU=OU_example,DC=example,DC=com`, для аутентификации оркестратора в LDAP-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 для аутентификации оркестратора в LDAP-сервере.

12. При необходимости убедиться в доступности LDAP-сервера нажмите на кнопку **Проверить аутентификацию**.

13. Нажмите на кнопку **Создать**.

LDAP-подключение будет создано и отобразится в таблице. Теперь LDAP-сервер можно использовать при создании пользователей или групп пользователей.

Изменение LDAP-подключения

Чтобы изменить LDAP-подключение:

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

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

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

   Отобразится таблица LDAP-подключений.

3. Нажмите на LDAP-подключение.

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

5. Нажмите на кнопку **Сохранить**.

Изменение пароля LDAP-подключения

Чтобы изменить пароль LDAP-подключения:

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

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

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

   Отобразится таблица LDAP-подключений.

3. Нажмите на LDAP-подключение.

4. Вверху отобразившейся области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Изменить пароль**.

5. В открывшемся окне в поле **Новый пароль** введите новый пароль. Пароль должен содержать как минимум один прописной символ A-Z, строчные символы, цифры, а также специальные символы. Длина пароля: от 8 до 50 символов.

6. В поле **Подтверждение пароля** повторно введите новый пароль.

7. Нажмите на кнопку **Сохранить**.

Пароль LDAP-подключения будет изменен.

Удаление LDAP-подключения

Удаленные LDAP-подключения невозможно восстановить.

Чтобы удалить LDAP-подключение:

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

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

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

   Отобразится таблица LDAP-подключений.

3. Нажмите на LDAP-подключение.

4. Вверху отобразившейся области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Удалить**.

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

LDAP-подключение будет удалено и перестанет отображаться в таблице.

Создание права доступа

Права доступа определяют, какие разделы и подразделы веб-интерфейса оркестратора доступны пользователям для просмотра и/или изменения параметров. По умолчанию в решении создано право доступа **Full access**, которое предоставляет пользователям полный доступ к управлению решением.

Чтобы создать право доступа:

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

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

2. Выберите вкладку **Права доступа**.

   Отобразится таблица прав доступа.

3. Вверху страницы 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** укажите уровень доступа пользователей к разделам и подразделам веб-интерфейса оркестратора:

   - **Изменение** – пользователи могут просматривать раздел/подраздел и вносить изменения в его параметры.

   - **Просмотр** – пользователи могут только просматривать раздел/подраздел.

- **Нет доступа** – пользователи не могут просматривать раздел/подраздел.

Вы можете предоставить выбранный уровень доступа ко всем подразделам внутри раздела, установив флажок **Применить к подразделам** рядом с этим разделом. По умолчанию флажок снят.

6. Нажмите на кнопку **Создать**.

Право доступа будет создано и отобразится в таблице. Теперь его можно использовать при создании пользователей или групп пользователей.

Изменение права доступа

Чтобы изменить право доступа:

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

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

2. Выберите вкладку **Права доступа**.

   Отобразится таблица прав доступа.

3. Нажмите на право доступа.

4. В отобразившейся области настройки измените требуемые параметры. Описание параметров см. в инструкции по созданию права доступа.

5. Нажмите на кнопку **Сохранить**.

Клонирование права доступа

Чтобы клонировать право доступа:

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

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

2. Выберите вкладку **Права доступа**.

   Отобразится таблица прав доступа.

3. Нажмите на право доступа.

4. Вверху отобразившейся области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **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 таблице.

Удаление права доступа

Удаленные права доступа невозможно восстановить.

Чтобы удалить право доступа:

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

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

2. Выберите вкладку **Права доступа**.

   Отобразится таблица прав доступа.

3. Нажмите на право доступа.

4. Вверху отобразившейся области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Удалить**.

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

Право доступа будет удалено и перестанет отображаться в таблице.

Создание пользователя

Вы можете создать пользователей, чтобы они могли аутентифицироваться в веб-интерфейсе оркестратора и управлять решением. Если вы хотите создать пользователя, который будет проходить аутентификацию через удаленный LDAP-сервер, перед выполнением этой инструкции требуется создать LDAP-подключение.

Чтобы создать пользователя:

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

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

2. Вверху страницы нажмите на кнопку **+ Пользователь**.

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

   - **Локальный** – пользователь, который аутентифицируется с помощью учетных данных, хранящихся локально в базе данных Kaspersky SD-WAN. Это значение выбрано по умолчанию.

   - **LDAP** – пользователь, который аутентифицируется с помощью учетных данных, хранящихся на удаленном LDAP-сервере.

4. В поле **Имя пользователя** введите локальное имя пользователя или имя пользователя на LDAP-сервере. Формат имени пользователя на LDAP-сервере: user@domain или domain\user.

5. При необходимости в полях **Пароль** и **Подтверждение пароля** введите локальный пароль пользователя. Пароль должен содержать как минимум один прописной символ A-Z, строчные символы, цифры, а также

специальные символы. Длина пароля: от 8 до 50 символов. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра 👁.

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

   - **Администратор** – пользователь имеет доступ ко всему решению.
   - **Тенант** – пользователь имеет доступ только к тенанту, которому вы его назначаете.

7. При необходимости в раскрывающемся списке **Права доступа** выберите право доступа для пользователя.

8. При необходимости создать запрос на подтверждение при каждом действии пользователя, установите флажок **Требуется подтверждение запроса**. По умолчанию флажок снят, и пользователь может свободно вносить любые изменения в параметры компонентов решения.

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

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

11. При необходимости в поле **Email** введите адрес электронной почты пользователя.

12. При необходимости в поле **Описание** введите краткое описание пользователя.

13. Нажмите на кнопку **Создать**.

Пользователь будет создан и отобразится в таблице.

Изменение пользователя

Чтобы изменить пользователя:

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

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

2. Нажмите на пользователя.

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

4. Нажмите на кнопку **Сохранить**.

Изменение пароля пользователя

Чтобы изменить пароль пользователя:

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

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

2. Нажмите на пользователя.

3. Вверху отобразившейся области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Изменить пароль**.

4. В открывшемся окне в поле **Новый пароль** введите новый пароль. Пароль должен содержать как минимум один прописной символ A-Z, строчные символы, цифры, а также специальные символы. Длина пароля: от 8 до 50 символов. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра .

5. В поле **Подтверждение пароля** повторно введите новый пароль.

6. Нажмите на кнопку **Сохранить**.

Пароль пользователя будет изменен.

Разблокировка и блокировка пользователя

По умолчанию созданные пользователи заблокированы. Вам нужно разблокировать пользователя, чтобы этот пользователь мог аутентифицироваться в веб-интерфейсе оркестратора.

Чтобы разблокировать или заблокировать пользователя:

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

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

2. Нажмите на пользователя.

3. Вверху отобразившейся области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Разблокировать** или **Заблокировать**.

Пользователь будет разблокирован или заблокирован.

Удаление пользователя

Удаленных пользователей невозможно восстановить.

Чтобы удалить пользователя:

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

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

2. Нажмите на пользователя.

3. Вверху отобразившейся области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Удалить**.

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

Пользователь будет удален и перестанет отображаться в таблице.

Создание группы пользователей

Вы можете создать группу пользователей, соответствующую группе на LDAP-сервере. Пользователи из этой группы смогут аутентифицироваться в веб-интерфейсе оркестратора. Обратите внимание, что добавление пользователей в группу осуществляется на LDAP-сервере без задействования оркестратора.

Перед созданием группы пользователей требуется выполнить следующие действия:

- создать группу пользователей на LDAP-сервере;
- настроить подключение оркестратора к LDAP-серверу.

Чтобы создать группу пользователей:

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

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

2. Выберите вкладку **Группы**.

   Отобразится таблица групп пользователей.

3. Вверху страницы нажмите на кнопку **+ Группа пользователей**.

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

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

   - **Администратор** – пользователи в группе имеют доступ ко всему решению.
   - **Тенант** – пользователи в группе имеют доступ только к тенанту, которому вы ее назначаете.

6. При необходимости в раскрывающемся списке **Права доступа** выберите право доступа для группы пользователей.

7. Нажмите на кнопку **Создать**.

Группа пользователей будет создана и отобразится в таблице.

Изменение группы пользователей

Чтобы изменить группу пользователей:

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

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

2. Выберите вкладку **Группы**.

   Отобразится таблица групп пользователей.

3. Нажмите на группу пользователей.

4. В отобразившейся области настройки измените требуемые параметры. Описание параметров см. в инструкции по созданию группы пользователей.

5. Нажмите на кнопку **Сохранить**.

Удаление группы пользователей

Удаленные группы пользователей невозможно восстановить.

Чтобы удалить группу пользователей:

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

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

2. Выберите вкладку **Группы**.

   Отобразится таблица групп пользователей.

3. Нажмите на группу пользователей.

4. Вверху отобразившейся области настройки нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Удалить**.

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

Группа пользователей будет удалена и перестанет отображаться в таблице.

Управление тенантами

Тенанты логически разделяют и изолируют объекты внутри сети SD-WAN. Каждый тенант определяет собственные политики управления и конфигурации и имеет полный контроль над собственными сетями и приложениями.

В рамках *мультитенантной* сети несколько независимых организаций, подразделений или клиентов используют одну физическую инфраструктуру и имеют собственные виртуальные сети. При этом один тенант не может получить доступ к сетевым ресурсам, назначенным другому тенанту. Несколько тенантов могут делить одно пространство IP-адресов.

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 последующих тенантов, выполните следующие действия:

   a. Вверху блока **Тенанты** нажмите на кнопку **+ Тенант**.

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

4. При необходимости в блоке внизу страницы введите краткое описание тенанта.

5. Нажмите на кнопку создания +

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

Назначение тенанту VIM

Чтобы назначить тенанту VIM:

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

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта.

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

4. В открывшемся окне выберите VIM. Для выбора VIM вам нужно сначала выбрать домен и ЦОД, в котором развернут этот VIM.

5. Нажмите на кнопку **Сохранить**.

Назначенный тенанту VIM отобразится в блоке **VIM**.

Назначение тенанту компонентов топологии

Чтобы назначить тенанту компоненты топологии:

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

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта.

3. В блоке **Каталог** установите флажки рядом с компонентами топологии, которые требуется назначить тенанту.

Компоненты топологии будут назначены тенанту и отобразятся в каталоге тенанта после обновления страницы.

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.

3. Вверху блока **Ресурсы** нажмите на кнопку 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 требуется назначить тенанту.

6. Нажмите на кнопку сохранения .

Назначение тенанту пользователя

Чтобы назначить тенанту пользователя:

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

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта.

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

4. В открывшемся окне выберите пользователя, которого требуется назначить тенанту.
5. Нажмите на кнопку **Сохранить**.

Назначенный тенанту пользователь 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.
3. В блоке **Группы пользователей** нажмите на кнопку **+ Изменить**.
4. В открывшемся окне выберите группу пользователей, которую требуется назначить тенанту.
5. Нажмите на кнопку **Сохранить**.

Назначенная тенанту группа пользователей отобразится в блоке **Группы пользователей**.

Аутентификация в веб-интерфейсе оркестратора тенанта в качестве администратора

Чтобы аутентифицироваться в веб-интерфейсе оркестратора тенанта в качестве администратора:

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

   Отобразится страница управления тенантами.
2. В блоке **Тенанты** выберите тенанта.
3. Нажмите на кнопку **Подключиться как тенант**.

Веб-интерфейс оркестратора тенанта откроется в новой вкладке браузера и вы будете аутентифицированы в нем как администратор.

Изменение тенанта

Чтобы изменить тенанта:

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

   Отобразится страница управления тенантами.
2. В блоке **Тенанты** нажмите на кнопку настройки рядом с тенантом и в раскрывающемся списке выберите **Изменить**.
3. Измените требуемые параметры. Описание параметров см. в инструкции по созданию тенанта.

4. В блоке, который отображается внизу страницы, нажмите на кнопку сохранения ✓.

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 кнопку настройки ⚙ рядом с тенантом и в раскрывающемся списке выберите **Удалить**.

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

Тенант будет удален и перестанет отображаться в блоке **Тенанты**.

Управление экземплярами SD-WAN

Экземпляром SD-WAN (англ. SD-WAN instance) является решение Kaspersky SD-WAN, развернутое на нескольких физических и/или виртуальных устройствах для одного тенанта. Экземпляр обеспечивает работу всех основных функций решения, таких как интеллектуальное управление трафиком и защита передаваемых данных. Он настраивается в соответствии с требованиями организации к необходимым уровням гибкости, безопасности и производительности при передаче данных через WAN-сеть.

Для централизованной настройки параметров экземпляров SD-WAN используются *шаблоны экземпляров SD-WAN*. Вы можете указать все параметры в одном шаблоне экземпляра SD-WAN, после чего использовать его при развертывании экземпляров для отдельных тенантов, таким образом избегая необходимости в их индивидуальной настройке. Тенанта необходимо добавить в шаблон экземпляра SD-WAN, чтобы этот шаблон использовался при развертывании экземпляра для тенанта.

Когда вы разворачиваете Kaspersky SD-WAN в первый раз, в веб-интерфейсе оркестратора автоматически создается шаблон экземпляра SD-WAN по умолчанию. Его невозможно удалить, но вы можете выбрать другой шаблон по умолчанию.

> Если вы развертываете решение для тенанта, который не добавлен ни в один шаблон экземпляра SD-WAN, к нему применяется шаблон по умолчанию.

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 SD-WAN, которое отличается от реального количества узлов у тенанта.

Вы можете сгруппировать экземпляры SD-WAN в пулы для обеспечения их масштабируемости и отказоустойчивости, особенно в условиях использования большого количества устройств.

Каждый *пул экземпляров SD-WAN* является балансировщиком нагрузки, где нагрузкой выступают устройства CPE. Во время создания устройства CPE его можно назначить пулу экземпляров SD-WAN или отдельным экземплярам из этого пула. Если вы назначаете устройство пулу экземпляров SD-WAN, оркестратор автоматически выбирает из этого пула экземпляр SD-WAN с наименьшим количеством устройств и назначает ему создаваемое устройство. При совпадении количества устройств экземпляр SD-WAN выбирается случайно.

Создание шаблона экземпляра SD-WAN

Чтобы создать шаблон экземпляра SD-WAN:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Вверху страницы нажмите на кнопку **+ Шаблон экземпляра SD-WAN**.

   Откроется подраздел **Шаблоны экземпляров SD-WAN**, в котором отображается таблица шаблонов экземпляров SD-WAN. Шаблон будет создан и отобразится в таблице. По умолчанию шаблону присваивается имя в формате Template <порядковый номер шаблона>.

Назначение шаблона экземпляра SD-WAN по умолчанию

Чтобы назначить шаблон экземпляра SD-WAN по умолчанию:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Назначить шаблоном по умолчанию**.

Удаление шаблона экземпляра SD-WAN

Вы не можете удалить шаблон экземпляра SD-WAN по умолчанию. Удаленные шаблоны невозможно восстановить.

Чтобы удалить шаблон экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху 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.

Добавление тенанта в шаблон экземпляра SD-WAN

Перед добавлением тенанта в шаблон экземпляра SD-WAN требуется создать тенанта и шаблон экземпляра SD-WAN.

Чтобы добавить тенанта в шаблон экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Тенанты**.

   Отобразится таблица тенантов.

4. Нажмите на кнопку **+ Тенант**.

5. В открывшемся окне выберите тенанта и нажмите на кнопку **Добавить**.
6. Вверху нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Тенант будет добавлен в шаблон экземпляра SD-WAN и отобразится в таблице.

Удаление тенанта из шаблона экземпляра SD-WAN

Чтобы удалить тенанта из шаблона экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.
2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.
3. Выберите вкладку **Тенанты**.

   Отобразится таблица тенантов.
4. Нажмите на кнопку **Удалить** рядом с тенантом.
5. Вверху нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Тенант будет удален из шаблона экземпляра SD-WAN и перестанет отображаться в таблице.

Настройка высокой доступности (high availability)

Архитектура решения предоставляет возможность сохранять высокую доступность (англ. high availability) экземпляров SD-WAN в случае прекращения работы или перегрузки виртуальных машин, устройств CPE, а также контроллеров SD-WAN. Высокая доступность этих компонентов обеспечивается установкой резервных устройств и соединений между ними.

Мы рекомендуем учитывать необходимость в высокой доступности компонентов решения при развертывании экземпляра SD-WAN.

Чтобы настроить высокую доступность:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.
2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.
3. Выберите вкладку **Высокая доступность**.

   Отобразятся параметры высокой доступности.
4. Выберите количество узлов контроллера SD-WAN, которое требуется использовать при развертывании экземпляра SD-WAN.

5. Вверху нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Выбор транспортной стратегии

Транспортная стратегия – это 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.

Чтобы выбрать транспортную стратегию:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Транспортная/сервисная стратегия**.

   Отобразится выбранная транспортная стратегия.

4. Убедитесь, что в раскрывающемся списке выбрана транспортная стратегия **Generic VNI swapping transport**.

Добавление тенанта в экземпляр SD-WAN

По умолчанию экземпляр SD-WAN развертывается для одного тенанта, но вы можете добавить других тенантов в уже развернутый экземпляр. В этом случае экземпляр осуществляет связность между устройствами CPE, назначенными добавленным в него тенантам. При добавлении тенанта вы также можете ограничить количество доступных ему устройств.

Перед добавлением тенанта в экземпляр SD-WAN требуется создать тенанта.

Чтобы добавить тенанта в экземпляр SD-WAN:

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

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Самообслуживание тенанта**.

   Отобразится таблица тенантов.

4. Нажмите на кнопку **+ Добавить**.

5. В открывшемся окне выберите тенанта.

6. В поле **Максимум CPE** введите максимальное количество доступных для тенанта устройств.

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 подраздел **SD-WAN → Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Самообслуживание тенанта**.

   Отобразится таблица тенантов.

4. Нажмите на кнопку **Удалить** рядом с тенантом.

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

Тенант будет удален из экземпляра SD-WAN и перестанет отображаться в таблице.

Просмотр устройств, назначенных экземпляру SD-WAN

Чтобы просмотреть устройства, назначенные экземпляру SD-WAN:

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

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Показать связанные CPE**.

Откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE. В таблице отобразятся только назначенные экземпляру SD-WAN устройства.

Удаление экземпляра SD-WAN

При удалении экземпляра также удаляются все назначенные ему устройства CPE и сетевой сервис, в котором он был развернут.

Альтернативным способом удаления экземпляра является удаление сетевого сервиса, в котором он был развернут. Удаленные экземпляры SD-WAN невозможно восстановить.

Чтобы удалить экземпляр SD-WAN:

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

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху 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.

Создание пула экземпляров SD-WAN

Чтобы создать пул экземпляров SD-WAN:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Вверху страницы нажмите на кнопку **+ Пул экземпляров SD-WAN**.

3. В открывшемся окне введите имя пула экземпляров SD-WAN.

4. Нажмите на кнопку **Создать**.

Откроется подраздел **Пулы экземпляров SD-WAN**, в котором отображается таблица пулов экземпляров SD-WAN. Пул экземпляров SD-WAN будет создан и отобразится в таблице. Теперь в него необходимо добавить экземпляры SD-WAN.

Добавление экземпляра SD-WAN в пул

Перед добавлением экземпляра SD-WAN в пул требуется создать пул экземпляров SD-WAN.

Чтобы добавить экземпляр SD-WAN в пул:

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

   Отобразится таблица пулов экземпляров SD-WAN.

2. Нажмите на пул экземпляров SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

4. Нажмите на кнопку **+ Экземпляр SD-WAN**.

5. В открывшемся окне выберите экземпляр SD-WAN, который требуется добавить в пул.

6. Нажмите на кнопку **Добавить**.

7. Вверху нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию пула экземпляров SD-WAN.

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

Удаление экземпляра SD-WAN из пула

Чтобы удалить экземпляр SD-WAN из пула:

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

   Отобразится таблица пулов экземпляров SD-WAN.

2. Нажмите на пул экземпляров SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Экземпляры SD-WAN**.

   Отобразится таблица экземпляров SD-WAN.

4. Нажмите на кнопку **Удалить** рядом с экземпляром SD-WAN.

   Экземпляр SD-WAN будет удален из пула и перестанет отображаться в таблице.

5. Вверху нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию 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 подраздел **SD-WAN** → **Пулы экземпляров SD-WAN**.

   Отобразится таблица пулов экземпляров SD-WAN.

2. Нажмите на пул экземпляров SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху 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

Kaspersky SD-WAN позволяет устанавливать в филиалах вашей организации или на клиентских площадках устройства CPE, обладающие следующими техническими характеристиками:

- Стандартная архитектура процессора:
  - x86 (Intel 80x86);
  - Arm v8/64 (Advanced RISC Machine);
  - MIPS (Microprocessor without Interlocked Pipeline Stages).
- Отсутствие зависимости от определенных производителей.
- Минимальные характеристики аппаратных ресурсов, таких как процессор и операционная память.

Подключаемые устройства CPE автоматически регистрируются в инвентаризационной базе данных и имеют прямой доступ в интернет (англ. Direct Internet Access, DIA). Вы можете использовать устройства CPE двух типов:

- Стандартные устройства CPE – для предоставления дополнительных VNF из ЦОД или облака вам нужно встроить виртуальное устройство CPE в сервисную цепочку. После предоставления VNF трафик передается к месту назначения.
- Universal CPE (далее также uCPE) – локальное размещение VNF улучшает время отклика, оптимизирует транспортные потоки и сохраняет возможность управлять этими VNF через веб-интерфейс оркестратора.

Состав устройств CPE

Устройства CPE имеют следующие внешние интерфейсы:

- Один или несколько LAN-интерфейсов. Вы можете объединить LAN-интерфейсы в коммутатор с помощью Linux-мостов. Это позволяет быстрее передавать данные на подключенные к коммутатору сетевые устройства, оптимизировать использование сетевых ресурсов и предотвратить появление узких мест (англ. bottlenecks).

  При отказе одного интерфейса трафик может быть передан на другой сохранивший работоспособность интерфейс. Объединение интерфейсов в один коммутатор также упрощает масштабирования сети, так как вы можете добавить новые интерфейсы в коммутатор при необходимости.
- Один или несколько WAN-интерфейсов. Эти интерфейсы могут иметь проводную или беспроводную среду передачи.

На каждом устройстве CPE существует программный коммутатор OpenFlow (англ. virtual switch, далее также программный коммутатор), который находится под управлением контроллера SD-WAN и по умолчанию имеет интерфейсы со следующими номерами:

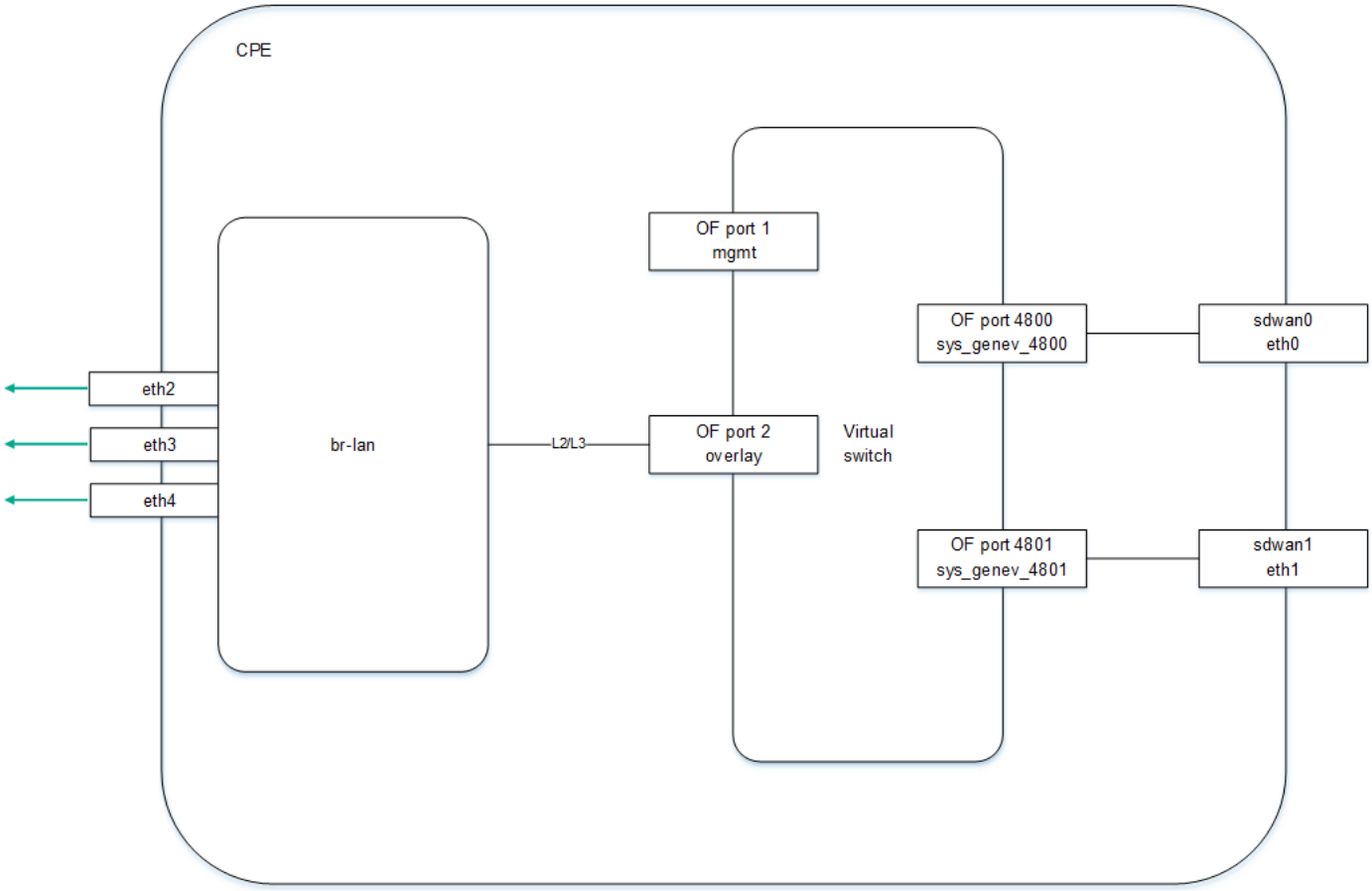
- 1 (ovs-mgmt) – обеспечивает организацию внутреннего управления сетью и настройку устройства CPE через управляющий транспортный сервис SD-WAN managementTunnel после подключения к оркестратору и контроллеру SD-WAN.
- 2 (ovs-lan) – обеспечивает подключение к Linux-мосту.

- 4800–4803 – GENEVE-интерфейсы, созданные для каждого WAN-интерфейса SD-WAN. Первый GENEVE-интерфейс имеет номер 4800. Другим GENEVE-интерфейсам присваиваются следующие по порядку номера. Например, второму GENEVE-интерфейсу присваивается номер 4801.

  В качестве IP-адреса источника требуется назначить IP-адрес соответствующего WAN-интерфейса. Интерфейсу назначения нужно присвоить номер GENEVE-интерфейса.

После того, как устройство CPE получает параметры WAN-интерфейсов, для каждого из них создается отдельная таблица маршрутизации.

На рисунке ниже изображена логическая схема устройства CPE.



Логическая схема устройства CPE

Состав устройств uCPE

Устройство uCPE дополнительно поддерживает развертывание VNF (как в виртуальной инфраструктуре ЦОД). Для установки программного обеспечения uCPE требуется сервер с архитектурой процессора x86. В состав каждого такого устройства входят гипервизор и VIM (OpenStack в минимальной конфигурации). Остальные компоненты, необходимые для оркестрации VNF, находятся в ЦОД. Программный коммутатор на устройстве uCPE содержит дополнительный интерфейс OS-data.

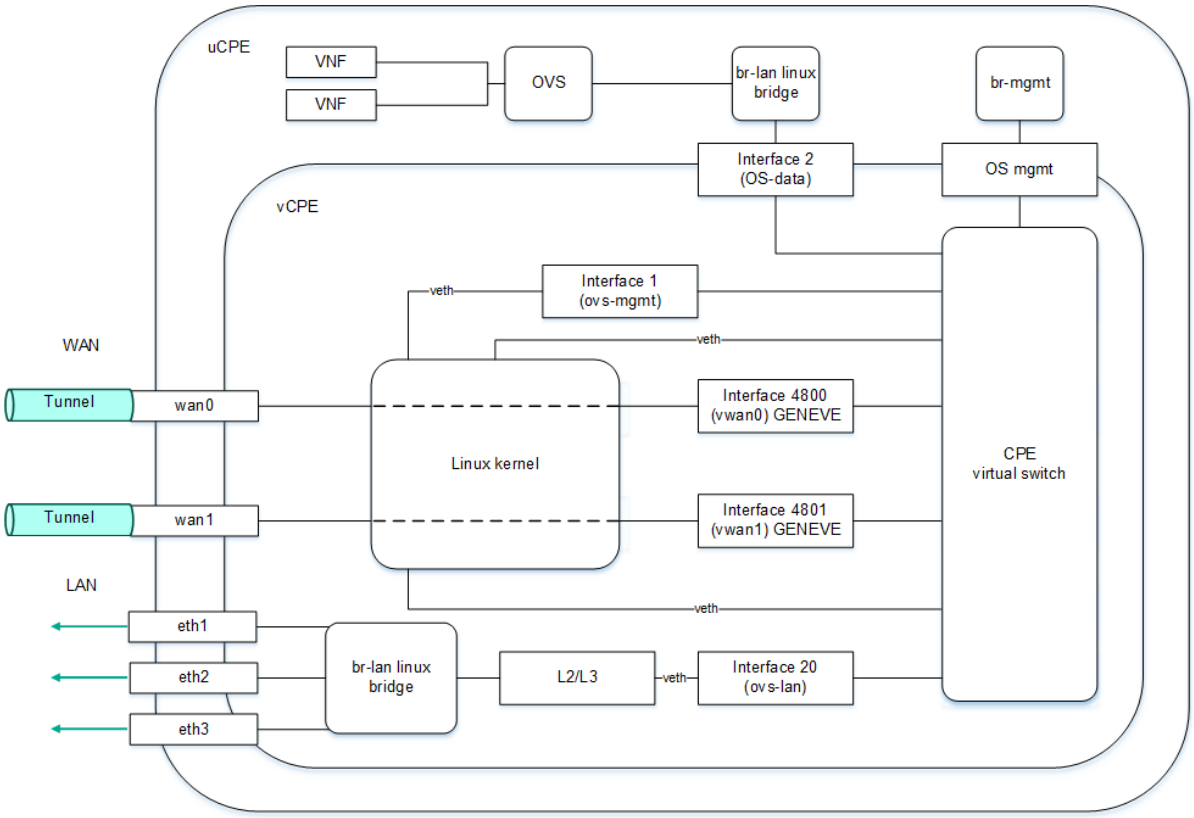
Оркестратор начинает взаимодействовать с VIM на устройстве uCPE после того, как это оно регистрируется и подключается к управляющему транспортному сервису SD-WAN managementTunnel.

Вы можете создать сетевой сервис на устройстве uCPE, которое находится в состоянии *Отключено*. В этом случае оркестратор отслеживает доступность устройства uCPE и создает сетевой сервис в момент, когда VIM начинает отвечать на API-запросы.

VIM на устройстве uCPE по умолчанию привязывается к тенанту, для которого развернут экземпляр SD-WAN, но вы можете выбрать другого тенанта.

При создании сетевого сервиса вам нужно выбрать VIM для развертывания VNF. Вы можете выбрать VIM в ЦОД, который привязан к тенанту, или VIM на устройстве uCPE. Если вы удалите устройство uCPE, все сервисные цепочки, развернутые на этом устройстве, будут удалены.

На рисунке ниже изображена логическая схема устройства uCPE.

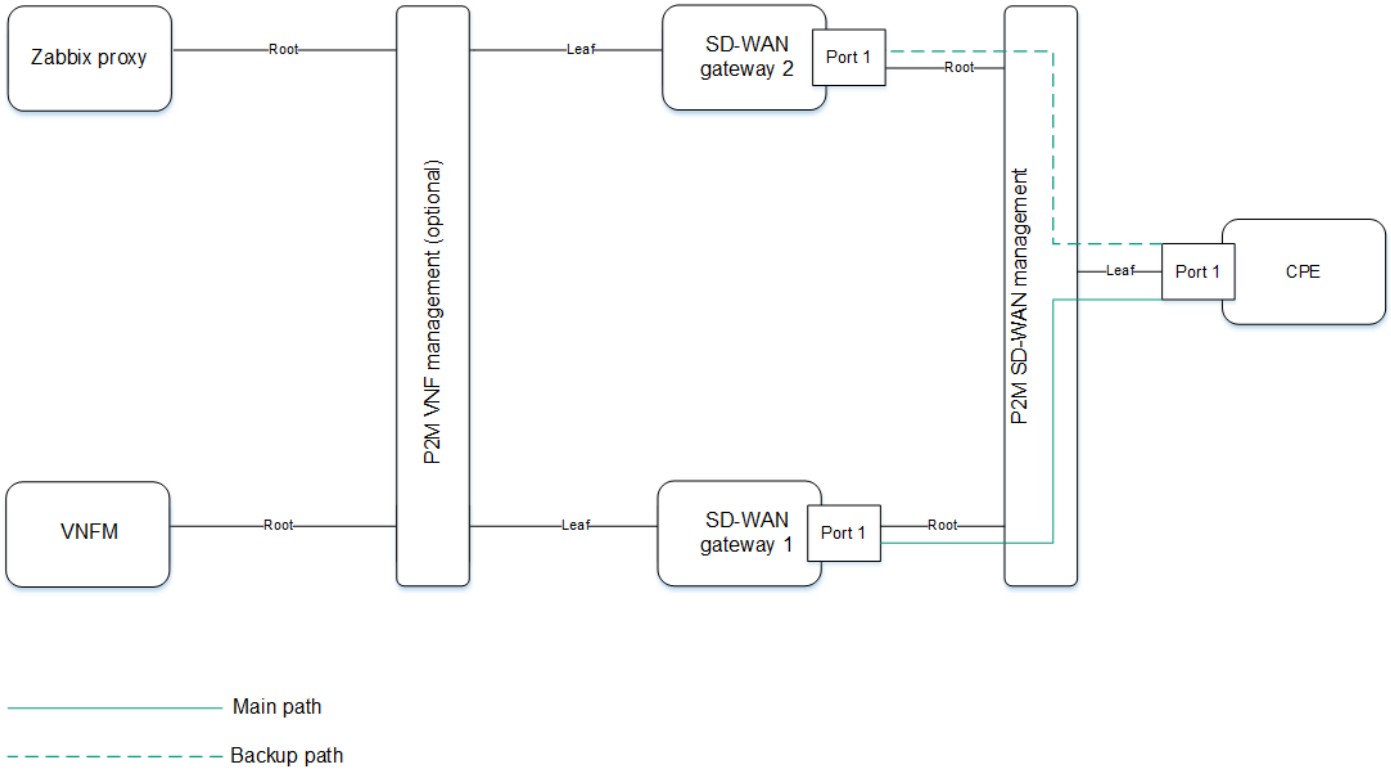


Логическая схема устройства uCPE

Управляющий транспортный сервис SD-WAN managementTunnel

Для управления устройствами CPE и их мониторинга Kaspersky SD-WAN использует P2M транспортный сервис SD-WAN managementTunnel. Корневыми интерфейсами этого транспортного сервиса являются сервисные интерфейсы на одном или нескольких устройствах CPE, за которыми находятся компоненты плоскости управления сетью.

После того, как устройство CPE подключается к контроллеру SD-WAN, поверх OpenFlow-интерфейса ovs-mgmt автоматически создается сервисный интерфейс с типом инкапсуляции Access. Оркестратор активирует устройство CPE и добавляет этот сервисный интерфейс в управляющий транспортный сервис SD-WAN managementTunnel с ролью Leaf (см. рисунок ниже).



Транспортный сервис управления устройством CPE

IP-адрес, необходимый для управления устройством CPE, определяется автоматически из заданного вами пула адресов. При удалении устройства CPE привязанный к нему IP-адрес возвращается в пул адресов. Компоненты VNF и PNF взаимодействуют друг с другом и с оркестратором с помощью внешних IP-адресов.

Вы можете предоставить доступ к веб-консоли устройства CPE и настроить подключение к консоли по протоколу SSH с помощью шаблона CPE. Обратите внимание, что для этого вам не нужно настраивать IP-связность с устройством.

VNFM предоставляет доступ к консоли устройства через управляющий транспортный сервис SD-WAN managementTunnel.

Автоматическая настройка устройств CPE (ZTP)

Каждое устройство CPE имеет уникальный *идентификатор DPID* (Datapath Identifier). Это 64-битное число, которое генерируется на основании уникальной характеристики устройства CPE, например MAC-адреса интерфейса WAN0 или серийного номера.

Для использования устройства CPE вам нужно сначала создать для него запись в веб-интерфейсе, после чего подключить само устройство к оркестратору. Альтернативным вариантом является подключение устройства к оркестратору (в этом случае в веб-интерфейсе оно отобразится со статусом *Неизвестно*) и последующее создание записи. В обоих случаях сопоставление записи с устройством происходит по идентификатору DPID.

Существует два основных сценария регистрации устройств CPE: с автоматической настройкой (англ. Zero Touch Provisioning, далее также ZTP) или с дополнительной конфигурацией. К дополнительной конфигурации, например относится назначение статических IP-адресов и создание маршрутов, загрузка сертификатов безопасности, а также генерация токенов.

Настройка устройства CPE осуществляется в следующей последовательности:

1. При необходимости дополнительной конфигурации используется URL-активация.
2. Устройство CPE получает IP-адреса WAN-интерфейсов и серверов DNS, а также маршруты по умолчанию от оператора связи по протоколу DHCP.
3. Устройство CPE использует FQDN или IP-адрес оркестратора, чтобы связаться с ним, сообщает свой идентификатор DPID, после чего получает внешние IP-адреса контроллера и шлюзов SD-WAN (при использовании). На него также загружаются сертификаты.
4. Устройство CPE устанавливает соединение с контроллером SD-WAN по протоколу TLS через IP-сеть, используя сеть оператора связи или интернет.
5. Контроллер SD-WAN программирует устройство CPE для создания туннелей от каждого WAN-интерфейса.

Для автоматической настройки устройства CPE через интернет требуется настроить внешние (англ. public) IP-адреса оркестратора, контроллера и шлюзов SD-WAN. В качестве альтернативы внешним IP-адресам поддерживается NAT для следующих интерфейсов:

- tcp 443, 81 для оркестратора.
- tcp 6653–6656 для контроллера SD-WAN.
- udp 4800–4803 для шлюзов SD-WAN.

Статусы и состояния устройства CPE

Устройства CPE могут иметь следующие статусы:

- *Неизвестно* – устройство подключено к оркестратору, но для него не создана запись в веб-интерфейсе.
- *Ожидание* – для устройства создана запись в веб-интерфейсе, но оно не подключено к оркестратору и/или не зарегистрировано.
- *Регистрация* – устройство находится в процессе регистрации.
- *Ошибка* – в процессе регистрации устройства возникла ошибка.
- *Зарегистрировано* – устройство успешно зарегистрировано.
- *Конфигурация* – на устройстве происходит изменение конфигурации.

Устройства CPE могут находиться в следующих состояниях:

- По отношению к оркестратору:
  - *Активировано* – к устройству применена конфигурация назначенного шаблона. Вы можете подключить такое устройство к транспортным сервисам и использовать его для передачи трафика.
  - *Деактивировано* (в статусе *Ожидание*) – к устройству не применена конфигурация назначенного шаблона. Вы можете внести локальные изменения в конфигурацию устройства перед тем как активировать его.

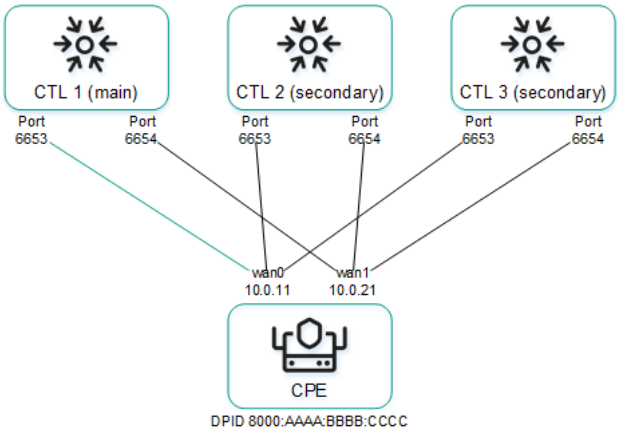
- *Деактивировано* (в статусе *Зарегистрировано*) – устройству заблокирована передача трафика по туннелям, и оркестратор не отвечает на поступающие от него запросы.

- По отношению к контроллеру SD-WAN:
  - *Активный* – устройство находится под управлением контроллера.
  - *Неактивный* –устройство не находится под управлением контроллера.

Обеспечение связности устройств CPE с контроллерами SD-WAN

Устройства CPE устанавливают соединение с контроллерами SD-WAN по протоколу OpenFlow в плоскости управления сетью через все WAN-интерфейсы: через каждый WAN-интерфейс устройства CPE устанавливается TCP-сессия ко всем контроллерам SD-WAN.

На схеме ниже изображен принцип установления соединений между устройством CPE и контроллерами SD-WAN.



Установление соединений между контроллерами SD-WAN и устройством CPE

В примере выше в кластере из трех контроллеров и устройства CPE с двумя WAN-интерфейсами устанавливается шесть TCP-сессий:

- 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

В один момент времени только одна сессия является основной (англ. primary session). Параметры переключения и восстановления основной сессии указываются при настройке подключения устройства CPE к сети SD-WAN.

Автоматическое изменение стоимости туннеля в зависимости от максимальной скорости интерфейса

Если скорость WAN-интерфейса SD-WAN на устройстве CPE выше скорости сети, предоставляемой оператором связи, вам нужно ограничить максимальную скорость этого интерфейса в соответствии со скоростью сети.

Пример:
Оператор связи предоставляет клиенту доступ в интернет на скорости 50 мегабит, а скорость физического подключения на интерфейсе устройства CPE составляет 100 мегабит. В этом случае для правильного расчета стоимости на туннелях и QoS необходимо указать значение максимальной скорости равным 50.

На основе параметра максимальной скорости высчитывается значение стоимости (англ. cost) на туннелях. Параметры максимальной скорости и стоимости связаны следующим образом:

- Максимальная скорость задает максимальную пропускную способность интерфейса для правильного расчета логических очередей для QoS. Измеряется в mbps (англ. megabits per second).
- Стоимость определяет вес интерфейса в топологии и рассчитывается по формуле `Cost = 10 000 000 / Speed`, где `Speed` равен значению максимальной скорости. Чем меньше значение стоимости, тем более приоритетным является туннель в топологии сети.

При изменении максимальной скорости значение стоимости меняется для туннелей в обоих направлениях. Для туннеля берется наименьшее значение максимальной скорости участвующих в нем интерфейсов.

Вы можете вручную указать стоимость туннеля, а также максимальную скорость интерфейса SD-WAN при его создании.

Шаблон CPE

Шаблон CPE содержит конфигурацию устройства CPE. Вы можете настроить конфигурацию в шаблоне один раз, после чего применять его к создаваемым устройствам. Таким образом, вы избегаете необходимости в индивидуальной настройке каждого отдельного устройства.

Обратите внимание, что определенные параметры устройства CPE можно настроить только в шаблоне. Например, в шаблоне указывается номер порта, который устройство будет использовать для подключения к оркестратору. Этот параметр невозможно изменить на отдельном устройстве.

Когда вы вносите изменения в конфигурацию шаблона CPE, они автоматически вносятся на всех использующих шаблон устройствах. После завершения работы с шаблоном CPE вы можете перейти к созданию и настройке отдельных устройств. Конфигурация устройства настраивается в соответствии с примененным шаблоном, однако в нее можно внести локальные изменения, если не все параметры соответствуют вашим требованиям.

Создание шаблона CPE

Чтобы создать шаблон CPE:

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

По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Вверху страницы нажмите на кнопку **+ Шаблон CPE**.
3. В открывшемся окне в поле **Имя** введите имя шаблона CPE.
4. В раскрывающемся списке **Тип** выберите тип шаблона CPE:
   - **CPE** – шаблон стандартного устройства CPE. Это значение выбрано по умолчанию.
   - **uCPE** – шаблон устройства uCPE.
5. Нажмите на кнопку **Создать**.

Откроется подраздел **Шаблоны CPE**, в котором отображается таблица шаблонов CPE. Шаблон будет создан и отобразится в таблице. Теперь его можно применить к устройству CPE при создании этого устройства.

Экспорт шаблона CPE

Вы можете экспортировать конфигурацию шаблона CPE, чтобы затем импортировать ее в другой шаблон.

Чтобы экспортировать шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Экспортировать**.

На ваше локальное устройство сохранится архив в формате TAR.GZ.

Архив содержит следующие данные:

- файл с описанием шаблона CPE в формате XML;
- файлы скриптов;
- файлы, необходимые для запуска скриптов, например SSL-сертификаты.

Конфигурация экспортируется полностью, включая все параметры, указанные на вкладках шаблона.

> В сохраненном архиве с конфигурацией не содержится информация об устройствах, к которым был применен оригинальный шаблон CPE.

Импорт шаблона CPE

Когда один шаблон CPE импортируется в другой, их конфигурация становится идентичной. Во время импорта вы можете выбрать вкладки шаблона CPE, на которых сохранится оригинальная конфигурация.

Перед импортом шаблона CPE требуется экспортировать шаблон CPE.

После импорта шаблон CPE останется примененным к устройствам, но конфигурация этих устройств не изменяется.

Чтобы импортировать шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Импортировать**.

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

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

6. Нажмите на кнопку **Импортировать**.

   Конфигурация шаблона CPE будет изменена в соответствии с конфигурацией импортируемого шаблона.

Клонирование шаблона CPE

При клонировании шаблона CPE создается его копия с новым именем, которая не применена ни к одному устройству.

Чтобы клонировать шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху 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 будет создана и отобразится в таблице.

Экспорт параметров и интерфейсов SD-WAN из шаблона CPE

Вы можете экспортировать из шаблона CPE параметры подключения устройства к сети SD-WAN, которые настраиваются на вкладке **Параметры SD-WAN**, а также конфигурацию интерфейсов SD-WAN, которые настраиваются на вкладке **Параметры SD-WAN → Интерфейсы**.

Чтобы экспортировать параметры и интерфейсы SD-WAN из шаблона CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху 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

Вы можете экспортировать из шаблона CPE конфигурацию сетевых интерфейсов, которые настраиваются на вкладке **Параметры сети**.

Чтобы экспортировать сетевые интерфейсы из шаблона CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Экспортировать сетевые интерфейсы**.

На ваше локальное устройство сохранится файл в формате JSON и именем <Имя шаблона>-network-config.

Просмотр устройств, использующих шаблон CPE

Чтобы просмотреть устройства, использующие шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Показать связанные CPE**.

   Откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE. В таблице отобразятся только использующие шаблон CPE устройства.

Удаление шаблона CPE

Вы не можете удалить шаблон, который применен к устройствам CPE. Удаленные шаблоны невозможно восстановить.

Чтобы удалить шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Вверху 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.

Создание устройства CPE

Перед подключением устройства CPE к оркестратору для него можно создать запись в веб-интерфейсе. Во время создания записи вам нужно указать идентификатор DPID, чтобы впоследствии сопоставить ее с подключаемым устройством. При успешном сопоставлении записи с устройством оно автоматически регистрируется.

Вы можете создать устройство CPE для текущего экземпляра SD-WAN, а также для выбранного тенанта или экземпляра SD-WAN. Для создания устройства CPE используйте следующие инструкции:

- Создание устройства CPE для текущего экземпляра SD-WAN

Чтобы создать устройство CPE для текущего экземпляра SD-WAN:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Вверху страницы нажмите на кнопку **+ CPE**.

3. В открывшемся окне в поле **Имя** введите имя устройства CPE.

4. В поле **DPID** введите идентификатор DPID устройства CPE.

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

   - **Активировано** – применить к устройству конфигурацию шаблона CPE. Активированное устройство можно подключать к транспортным сервисам и использовать для передачи трафика. Это значение выбрано по умолчанию.

   - **Деактивировано** – не применять к устройству конфигурацию шаблона CPE. Вы можете внести локальные изменения в конфигурацию устройства перед активацией.

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

7. В блоке **Тенант** выберите основного тенанта. Вы можете выбрать пул экземпляров SD-WAN или отдельный экземпляр из пула.

8. При необходимости в блоке **Клиентский тенант** выберите тенанта организации вашего клиента.

9. При необходимости в блоке **Шаблон UNI** выберите шаблон UNI, чтобы создать на устройстве содержащиеся в шаблоне UNI.

10. В блоке **Шаблон CPE** выберите шаблон CPE, чтобы настроить устройство в соответствии с конфигурацией этого шаблона.

11. 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.

12. Нажмите на кнопку **Создать**.

Устройство CPE будет создано и отобразится в таблице. Теперь его можно настроить, после чего использовать для передачи трафика.

- Создание устройства CPE для тенанта.

Чтобы создать устройство CPE для тенанта:

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

   Отобразится страница управления тенантами.

2. В блоке **Тенанты** выберите тенанта.

3. В блоке **Устройства CPE** нажмите на кнопку **+ Устройство CPE**.

4. В открывшемся окне в поле **Имя** введите имя устройства CPE.

5. В поле **DPID** введите идентификатор DPID устройства CPE.

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

   - **Активировано** – применить к устройству конфигурацию шаблона CPE. Активированное устройство можно подключать к транспортным сервисам и использовать для передачи трафика. Это значение выбрано по умолчанию.

   - **Деактивировано** – не применять к устройству конфигурацию шаблона CPE. Вы можете внести локальные изменения в конфигурацию устройства перед активацией.

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

8. При необходимости в блоке **Клиентский тенант** выберите тенанта организации вашего клиента.

9. При необходимости в блоке **Шаблон UNI** выберите шаблон UNI, чтобы создать на устройстве содержащиеся в шаблоне UNI.

10. В блоке **Шаблон CPE** выберите шаблон CPE, чтобы настроить устройство в соответствии с конфигурацией этого шаблона.

11. 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.

12. Нажмите на кнопку **Создать**.

Устройство CPE будет создано и отобразится в блоке **Устройства CPE**. Теперь его можно настроить, после чего использовать для передачи трафика.

- Создание устройства CPE для экземпляра SD-WAN.

Чтобы создать устройство CPE для экземпляра SD-WAN:

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

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху области настройки нажмите на кнопку **CPE**.

4. В открывшемся окне в поле **Имя** введите имя устройства CPE.

5. В поле **DPID** введите идентификатор DPID устройства CPE.

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

   - **Активировано** – применить к устройству конфигурацию шаблона CPE. Активированное устройство можно подключать к транспортным сервисам и использовать для передачи трафика. Это значение выбрано по умолчанию.

   - **Деактивировано** – не применять к устройству конфигурацию шаблона CPE. Вы можете внести локальные изменения в конфигурацию устройства перед активацией.

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

8. В блоке **Тенант** выберите основного тенанта. Вы можете выбрать пул экземпляров SD-WAN или отдельный экземпляр из пула.

9. При необходимости в блоке **Клиентский тенант** выберите тенанта организации вашего клиента.

10. При необходимости в блоке **Шаблон UNI** выберите шаблон UNI, чтобы создать на устройстве содержащиеся в шаблоне UNI.

11. В блоке **Шаблон CPE** выберите шаблон CPE, чтобы настроить устройство в соответствии с конфигурацией этого шаблона.

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 **Создать**.

    Веб-интерфейс экземпляра SD-WAN откроется в новой вкладке браузера и вы будете аутентифицированы как администратор. По умолчанию вы перейдете в подраздел **Устройства CPE**, в котором отображается таблица устройств CPE. Устройство будет создано и отобразится в таблице. Теперь его можно настроить, после чего использовать для передачи трафика.

Указание адреса устройства CPE

Чтобы указать адрес устройства CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху 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**.

Регистрация устройства CPE

Если устройство CPE подключается к оркестратору и не может быть сопоставлено ни с одной из созданных вами записей, его необходимо зарегистрировать. При регистрации устройства CPE не требуется подключаться к облачным сервисам производителя.

Чтобы зарегистрировать устройство CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Зарегистрировать**.

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

   - **Активировано** – применить к устройству конфигурацию шаблона CPE. Активированное устройство можно подключать к транспортным сервисам и использовать для передачи трафика. Это значение выбрано по умолчанию.

   - **Деактивировано** – не применять к устройству конфигурацию шаблона CPE. Вы можете внести локальные изменения в конфигурацию устройства перед активацией.

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

6. В блоке **Тенант** выберите основного тенанта. Вы можете выбрать пул экземпляров SD-WAN или отдельный экземпляр из пула.

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

8. При необходимости в блоке **Шаблон UNI** выберите шаблон UNI, чтобы создать на устройстве содержащиеся в шаблоне UNI.

9. В блоке **Шаблон CPE** выберите шаблон CPE, чтобы настроить устройство в соответствии с конфигурацией этого шаблона.

10. 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.

11. Нажмите на кнопку **Зарегистрировать**.

Статус устройства CPE изменится сначала на *Регистрация*, затем на *Зарегистрировано*.

Ваши дальнейшие действия определяются значением, выбранным в раскрывающемся списке **Состояние**:

- Если вы выбрали **Активировано**, вы можете использовать устройство для передачи трафика.
- Если вы выбрали **Деактивировано**, вам нужно настроить устройство, затем активировать, и только тогда вы сможете использовать его для передачи трафика.

Активация и деактивация устройства CPE

При активации устройства к нему применяется шаблон CPE. Не активированное устройство невозможно использовать для передачи трафика.

Чтобы активировать или деактивировать устройство CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Активировать** или **Деактивировать**.

Активация устройства CPE с помощью веб-адреса

Kaspersky SD-WAN поддерживает активацию устройств CPE с помощью веб-адреса (англ. URL-based ZTP). Активация с помощью веб-адреса упрощает и ускоряет первоначальную настройку CPE путем автоматизации передачи параметров конфигурации в адрес и последующего ее применения.

Минимизация ручного вмешательства при активации с помощью веб-адреса снижает требования к сотруднику, который активирует и настраивает устройство CPE на месте его установки. Этот способ активации удобен при двухфакторной аутентификации или первичном внесении базовых настроек сетевой связности для подключения устройства CPE к оркестратору (например, статических IP или BGP).

Существуют следующие особенности активации с помощью веб-адреса:

- Активация с помощью веб-адреса доступна для устройств CPE с прошивкой в стартовом состоянии.
- Устройства CPE не должно находиться в статусе *Неизвестно*.

Вы можете указать шаблон веб-адреса для активации при настройке подключения устройства CPE к сети SD-WAN в поле **URL ZTP**.

Чтобы активировать устройство CPE с помощью веб-адреса:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Получить URL активации** и в открывшемся окне скопируйте веб-адрес.

4. Отправьте веб-адрес пользователю, который активирует и настраивает устройство CPE на месте его установки. Пользователю нужно выполнить следующие действия, чтобы активировать устройство CPE:

   a. Подключиться к LAN-интерфейсу устройства CPE и получить IP-адрес по DHCP.

   b. Перейти по полученной ссылке или вставить веб-адрес в адресную строку браузера.

   c. Дождаться, пока устройство CPE получит конфигурацию, применит полученные параметры и перезагрузится.

Подключение к консоли устройства CPE

Чтобы подключиться к консоли устройства CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. В блоке **Действия** нажмите на кнопку **Открыть SSH-консоль**.

В новой вкладке браузера откроется окно консоли.

Удаление устройства CPE

Когда вы удаляете устройство CPE, автоматически удаляются все созданные на этом устройстве сервисные интерфейсы. Удаленные устройства CPE невозможно восстановить.

Чтобы удалить устройство CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Удалить**.

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

Устройство CPE будет удалено и перестанет отображаться в таблице.

Просмотр пароля устройства CPE

Чтобы просмотреть пароль устройства CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Показать пароль**.

Откроется окно с паролем устройства CPE.

Перезагрузка устройства CPE

Чтобы перезагрузить устройство CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Перезагрузить**.

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

Выключение устройства CPE

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

Чтобы выключить устройство CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Выключить**.

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

Экспорт параметров и интерфейсов SD-WAN из устройства CPE

Вы можете экспортировать из устройства CPE параметры подключения устройства к сети SD-WAN, которые настраиваются на вкладке **Параметры SD-WAN**, а также конфигурацию интерфейсов SD-WAN, которые настраиваются на вкладке **Параметры SD-WAN** → **Интерфейсы**.

Чтобы экспортировать параметры и интерфейсы SD-WAN из устройства CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху 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

Вы можете экспортировать из устройства CPE конфигурацию сетевых интерфейсов, которые настраиваются на вкладке **Параметры сети**.

Чтобы экспортировать сетевые интерфейсы из шаблона CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Вверху области настройки в блоке **Действия** нажмите на кнопку **Экспортировать сетевые интерфейсы**.

На ваше локальное устройство сохранится файл в формате JSON и именем <Имя шаблона>-network-config.

Поиск устройств CPE

Чтобы найти устройство CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Вверху страницы нажмите на кнопку поиска и в отобразившемся поле введите требуемый критерий поиска. Например, вы можете ввести имя устройства CPE, IP-адрес или один из назначенных тегов.

Результаты поиска отобразятся в таблице.

Автоматическое удаление и деактивация устройства CPE

Вы можете указать время, по прошествии которого отдельное устройство CPE или все устройства, использующие шаблон CPE будут удалены или деактивированы в случае потери связи с контроллером SD-WAN.

Обе функции используются для предотвращения краж устройств. Функция автоматического удаления также используется для очистки веб-интерфейса оркестратора от устаревших записей. По умолчанию обе функции выключены.

Для автоматического удаления и деактивации устройств CPE используйте следующие инструкции:

- **Настройка автоматического удаления и/или деактивации отдельного устройства CPE**.

Чтобы настроить автоматическое удаление и/или деактивацию отдельного устройства CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Деактивация**.

   Отобразятся параметры функций автоматического удаления и деактивации устройства CPE.

4. Настройте автоматическое удаление устройства CPE:

   a. Установите флажок **Переопределить** рядом с полем **Время удаления (сек.)**, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры автоматического удаления. По умолчанию флажок снят.

   b. Установите флажок **Включить** рядом с полем **Время удаления (сек.)**, чтобы включить автоматическое удаление.

   c. В поле **Время удаления (сек.)** введите время, по прошествии которого устройство требуется удалить при отсутствии связи с контроллером SD-WAN. Время указывается в секундах. Диапазон значений: от 60 до 31 536 000. Введенное значение не должно быть ниже значения, которое вы указываете для функции автоматической деактивации.

5. Настройте автоматическую деактивацию устройства CPE:

   a. Установите флажок **Переопределить** рядом с полем **Время деактивации (сек.)**, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры автоматической деактивации. По умолчанию флажок снят.

   b. Установите флажок **Включить** рядом с полем **Время деактивации (сек.)**, чтобы включить автоматическую деактивацию.

   c. В поле **Время деактивации (сек.)** введите время, по прошествии которого устройство требуется деактивировать при отсутствии связи с контроллером SD-WAN. Время указывается в секундах. Диапазон значений: от 60 до 31 536 000. Введенное значение не должно быть выше значения, которое вы указываете для функции автоматического удаления.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Настройка автоматического удаления и/или деактивации всех устройств, использующих шаблон CPE.

Чтобы настроить автоматическое удаление и/или деактивацию всех устройств, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Деактивация**.

   Отобразятся параметры функций автоматического удаления и деактивации устройства CPE.

4. Настройте автоматическое удаление всех устройств, использующих шаблон CPE:

   a. Установите флажок **Включить** рядом с полем **Время удаления (сек.)**, чтобы включить автоматическое удаление. По умолчанию автоматическое удаление выключено.

   b. В поле **Время удаления (сек.)** введите время, по прошествии которого устройство требуется удалить при отсутствии связи с контроллером SD-WAN. Время указывается в секундах. Диапазон значений: от 60 до 31 536 000. Введенное значение не должно быть ниже значения, которое вы указываете для функции автоматической деактивации.

5. Настройте автоматическую деактивацию всех устройств, использующих шаблон CPE:

   a. Установите флажок **Включить** рядом с полем **Время деактивации (сек.)**, чтобы включить автоматическую деактивацию. По умолчанию автоматическая деактивация выключена.

   b. В поле **Время деактивации (сек.)** введите время, по прошествии которого устройство требуется деактивировать при отсутствии связи с контроллером SD-WAN. Время указывается в секундах. Диапазон значений: от 60 до 31 536 000. Введенное значение не должно быть выше значения, которое вы указываете для функции автоматического удаления.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Двухфакторная аутентификация устройства CPE

Двухфакторная аутентификация используется для безопасной регистрации устройства CPE. При включении двухфакторной аутентификации в базу данных оркестратора записывается ключ безопасности, который вам нужно вручную ввести на устройстве. Регистрация проходит успешно только при условии совпадения двух ключей безопасности.

Чтобы настроить двухфакторную аутентификацию на устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Активация**.

   Отобразятся параметры двухфакторной аутентификации устройства CPE.

4. В раскрывающемся списке **Двухфакторная аутентификация** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

5. Если вы включили двухфакторную аутентификацию, нажмите на кнопку **Сгенерировать** под полем **Токен**, чтобы сгенерировать ключ безопасности.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

7. Введите сгенерированный ключ безопасности на устройстве CPE в папке /etc/config/sdwan.

Сертификаты оркестратора

Для предотвращения MITM-атак (англ. man in the middle) при обращении к оркестратору устройство CPE проверяет, можно ли доверять сертификату оркестратора. По умолчанию на устройствах установлены корневые сертификаты публичных центров сертификации.

Если для оркестратора используется сертификат, подписанный публичным центром сертификации, установка дополнительного сертификата на устройствах не требуется. В противном случае необходимо добавить используемый оркестратором публичный корневой сертификат на устройствах, загрузив его в веб-интерфейс оркестратора.

Существуют следующие особенности управления сертификатами:

- при каждой загрузке нового сертификата в веб-интерфейсе оркестратора сертификат распространяется на устройства CPE автоматически;
- при первоначальной активации устройства CPE с помощью веб-адреса загруженный в оркестратор сертификат автоматически устанавливается на устройстве;
- за 30 дней до окончания срока действия сертификата оркестратор начинает выводить уведомление об этом при каждой аутентификации пользователя в веб-интерфейсе оркестратора.

Загрузка сертификата оркестратора

Чтобы загрузить сертификат оркестратора:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Вверху страницы нажмите на кнопку **+ Сертификат**.

3. Укажите путь к файлу сертификата в формате PEM. Максимальный размер файла: 128 КБ.

Информация о загруженном сертификате отобразится в подразделе **Сертификат**. Сертификат будет автоматически распространен на устройствах CPE. Вы можете распространить сертификат вручную.

Просмотр сертификата оркестратора

Чтобы просмотреть сертификат оркестратора,

в меню перейдите в подраздел **SD-WAN → Сертификат**.

Откроется страница с информацией о загруженном сертификате оркестратора.

Распространение сертификата оркестратора на устройствах CPE вручную

Вы можете вручную распространить сертификат оркестратора на устройствах CPE, не дожидаясь автоматического распространения.

Чтобы распространить сертификат оркестратора на устройствах CPE вручную:

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

   Откроется страница с информацией о загруженном сертификате оркестратора.

2. Вверху страницы нажмите на кнопку **Применить к CPE**.

Экспорт сертификата оркестратора

Чтобы экспортировать сертификат оркестратора:

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

   Откроется страница с информацией о загруженном сертификате оркестратора.

2. Вверху страницы нажмите на кнопку **Экспортировать**.

На ваше локальное устройство сохранится файл в формате PEM с именем cacert.

Теги

Теги – это метки, которые описывают различные параметры устройства CPE, например модель, версию программного обеспечения или адрес расположения. Теги классифицируют устройства для выполнения с ними требуемых задач. Например, с их помощью вы можете сгруппировать устройства одной модели, после чего обновить на них прошивку.

Когда вы создаете устройство CPE ему автоматически назначаются теги, описывающие модель и тенанта, к которому оно относится.

Если требуется, вы можете назначить теги одному или нескольким устройствам CPE одновременно. Обратите внимание, что для назначения тега устройство должно находиться в статусе *Зарегистрировано*.

Kaspersky SD-WAN не поддерживает назначение двух одинаковых тегов одному устройству CPE.

Назначение тегов устройствам CPE

Чтобы назначить тег отдельному устройству CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Теги**.

   Отобразятся назначенные устройству CPE теги.

4. Введите тег и нажмите на кнопку назначения +.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы назначить тег нескольким устройствам CPE одновременно:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Установите флажки рядом с устройствами CPE.

3. Вверху страницы в раскрывающемся списке **Действия** выберите **Добавить теги**.

4. В открывшемся окне введите тег и нажмите на кнопку назначения +.

5. Нажмите на кнопку **Добавить**.

Удаление тегов устройств CPE

Чтобы удалить тег отдельного устройства CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Теги**.

   Отобразятся назначенные устройству CPE теги.

4. Нажмите на кнопку удаления ✕ рядом с тегом.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить тег нескольких устройств CPE одновременно:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Установите флажки рядом с устройствами CPE.

3. Вверху страницы в раскрывающемся списке **Действия** выберите **Удалить теги**.

4. В открывшемся окне удалите теги:

   - Нажмите на кнопку удаления ✕ рядом с тегом.
   - Введите тег в поле и выберите его в раскрывающемся списке.

5. Нажмите на кнопку **Удалить**.

Внеполосное управление устройствами CPE

В рамках развернутого Kaspersky SD-WAN взаимодействие оркестратора с устройствами CPE происходит через наложенную сеть SD-WAN и является *внутриполосным* (англ. in-band). Однако решение также поддерживает *внеполосное управление* (англ. out-of-band management, далее также OOB-управление), подразумевающее передачу управляющего трафика между оркестратором и устройствами через подлежащую (англ. underlay) сеть по HTTPS или TLS без задействования туннелей.

OOB-управление позволяет управлять устройствами CPE, а также проводить их диагностику, даже в случае отсутствия установленных туннелей. Например, вы можете использовать OOB-управление, если используете только точки подключения local breakout или при возникновении аварии на сети SD-WAN.

После регистрации устройство CPE начинает отправлять API-запросы оркестратору с определенным интервалом времени для получения новых конфигураций. Интервал времени указывается при настройке подключения устройства к сети SD-WAN в поле **Интервал обновления (сек.)**.

Когда вы вносите изменения в конфигурацию устройства CPE в веб-интерфейсе, оркестратор сохраняет новую конфигурацию со статусом *Ожидание*. Устройство в свою очередь получает эту конфигурацию при очередном отправлении API-запроса, и она переходит в статус *Выполнение*. В случае успешного применения конфигурации устройство сообщает об этом оркестратору, после чего она переходит в статус *Выполнено*. Если устройство сообщает о невозможности применения конфигурации, она переходит в статус *Ошибка*.

Перед применением новой конфигурации на устройстве CPE выполняется копирование текущей конфигурации. Если после успешного применения новой конфигурации устройство не может отправить оркестратору сообщение с подтверждением, после 3-х попыток выполняется откат к предыдущей версии. В этом случае конфигурация на оркестраторе также переходит в статус *Ошибка*.

Вы можете просматривать статусы конфигураций на отдельном устройстве CPE.

Чтобы просмотреть статус конфигураций:

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

По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃. Конфигурации и их статус отображаются в таблице **Внеполосное управление**.

Управление устройствами CPE через меню контроллера SD-WAN

Когда вы создаете устройство CPE, оно также отображается в разделе **Коммутаторы** меню настройки контроллера SD-WAN. В этом подразделе вы можете управлять устройством и просматривать на нем статистику. Устройства отображаются в таблице со следующими столбцами:

- **Имя** – имя устройства CPE.
- **ID** – порядковый номер устройства CPE. С помощью этого столбца вы можете определять, в каком порядке устройства подключились к контроллеру SD-WAN. Устройство с наименьшим порядковым номером подключилось к контроллеру первым.
- **Статус** – статус устройства CPE в контроллере SD-WAN. В этом столбце может отображаться один из следующих статусов:
  - *Активный* – устройство находится под управлением контроллера.
  - *Неактивный* –устройство не находится под управлением контроллера.
- **Подключение** – статус подключения устройства CPE к контроллеру SD-WAN. В этом столбце может отображаться один из следующих статусов:
  - *Подключен* – между устройством и контроллером установлена TCP-сессия.
  - *Отключен* – между устройством и контроллером не установлена TCP-сессия.
- **MAC** – MAC-адрес устройства CPE.
- **Интерфейс** – один или несколько WAN-интерфейсов SD-WAN устройства CPE для установления TCP-сессии с контроллером SD-WAN.
- **Основная сессия** – WAN-интерфейс SD-WAN устройства CPE, через который установлено управляющее соединение с контроллером SD-WAN.
- **IP** – IP-адрес, который устройство CPE использует для установления TCP-сессии с контроллером SD-WAN.
- **Порт** – номер порта, который устройство CPE использует для установления TCP-сессии с контроллером SD-WAN.
- **Создан** – дата и время регистрации устройства CPE.
- **Адрес** – адрес площадки устройства CPE.
- **Задержка (мс.)** – время задержки в миллисекундах для TCP-сессии между устройством CPE и контроллером SD-WAN. Отображается значение для управляющего соединения.

- **Описание** – краткое описание устройства CPE.

Обратите внимание, что отображающаяся вверху страницы кнопка **Коммутатор** не используется для создания новых устройств CPE. Это действие выполняется в разделе **SD-WAN**.

Просмотр статистики на устройствах CPE позволяет анализировать и контролировать процесс передачи трафика между этими устройствами и адаптировать используемые сетевые политики в соответствии с изменяющимися требованиями вашей организации.

Мы не рекомендуем изменять параметры устройств CPE и OpenFlow-интерфейсов в разделе **Коммутаторы**, так как это может привести к неполадкам в работе сети SD-WAN. Вы можете изменить параметры устройств CPE в подразделе **Устройства CPE**, а параметры OpenFlow-интерфейсов – в конфигурации устройства CPE на вкладке **Параметры SD-WAN**.

Просмотр OpenFlow-таблицы устройства CPE

Чтобы просмотреть OpenFlow-таблицу устройства CPE:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **OpenFlow-таблица**.

Откроется OpenFlow-таблица устройства CPE. Вы можете переключаться между страницами таблицы, используя кнопки **Предыдущая** и **Следующая**.

Просмотр статистики OpenFlow-интерфейсов

Чтобы просмотреть статистику OpenFlow-интерфейсов:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **Статистика интерфейса**.

   Откроется таблица статистики OpenFlow-интерфейсов.

5. При необходимости измените содержимое таблицы:

   - Вверху страницы нажмите на кнопку настройки и в раскрывающемся списке выберите параметры, которые требуется отобразить в статистике.
   - Нажмите на кнопку **Очистить статистику**, чтобы очистить статистику.

Просмотр статистики очередей на LAN-интерфейсах

Чтобы просмотреть статистику очередей на LAN-интерфейсах:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **Статистика очередей**.

Откроется таблица статистики очередей на LAN-интерфейсах.

Переход к сервисным интерфейсам на устройстве CPE

Чтобы перейти к сервисным интерфейсам, созданным на устройстве CPE:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **Сервисные интерфейсы**.

Откроется подраздел **Сервисные интерфейсы**, в котором отображается таблица сервисных интерфейсов.

Просмотр технических характеристик устройства CPE

Чтобы просмотреть технические характеристики устройства CPE:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **Информация об оборудовании**.

Откроется окно с техническими характеристиками устройства CPE.

Просмотр использования устройства CPE

Чтобы просмотреть компоненты Kaspersky SD-WAN, которые используют устройство CPE:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **Показать использование**.

Откроется окно, в котором отображается таблица компонентов решения, использующих устройство CPE.

Изменение статуса устройства CPE в контроллере SD-WAN

Чтобы изменить статус устройства CPE в контроллере SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **Включить** или **Выключить**.

Статус устройства CPE будет изменен на *Активный* или *Неактивный*.

Изменение MAC-адреса устройства CPE

Чтобы изменить MAC-адрес устройства CPE:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **Мигрировать**.

5. В открывшемся окне введите новый MAC адрес устройства CPE.

6. Нажмите на кнопку **Сохранить**.

Разрыв TCP-сессии между устройством CPE и контроллером SD-WAN

Чтобы разорвать TCP-сессию между устройством CPE и контроллером SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Коммутаторы**.

   Отобразится таблица устройств CPE.

4. Нажмите на кнопку **Управление** рядом с устройством CPE и в раскрывающемся списке выберите **Разорвать соединение**.

TCP-сессия между устройством CPE и контроллером SD-WAN будет разорвана.

Скрипты

Скрипт – это последовательность команд и инструкций, которые используются для настройки устройств CPE. Каждый скрипт изменяет один или несколько параметров устройства.

Вы можете добавить в шаблон CPE скрипты, которые запускаются автоматически или требуют ручного запуска. В обоих случаях скрипты запускает VNFM. Обратите внимание, что перед добавлением и запуском скриптов на устройстве необходимо настроить подключение VNFM к его консоли.

Автоматический запуск скриптов происходит при соблюдении условий, которые вы указываете в параметрах скрипта. Например, скрипт может автоматически запускаться при регистрации устройства CPE.

Настройка подключения VNFM к консоли устройства CPE

Запуск скриптов на устройстве CPE обеспечивает VNFM. В шаблоне CPE необходимо указать имя и пароль пользователя, а также номер SSH-порта, чтобы VNFM мог подключиться к консоли устройства и запускать скрипты. Указанные параметры подключения применяются ко всем устройствам, использующим шаблон. Подключение настраивается один раз, за исключением случаев, когда вам нужно использовать другого пользователя на устройстве CPE или изменить номер SSH-порта.

Чтобы настроить параметры подключения VNFM к консоли устройства CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Скрипты**.

   Отобразятся параметры подключения VNFM к консоли устройства CPE, а также таблица скриптов, если добавлен хотя бы один скрипт.

4. В поле **Имя пользователя по умолчанию** введите имя пользователя для аутентификации VNFM в консоли устройства. Максимальная длина: 255 символов.

5. В поле **SSH-порт** введите номер порта для подключения VNFM к консоли устройства CPE. По умолчанию указано значение `1`.

6. В поле **Пароль по умолчанию** введите пароль пользователя для аутентификации VNFM в консоли устройства CPE. Максимальная длина: 255 символов. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра .

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Добавление скрипта

Вы можете добавить скрипт только в шаблон CPE. Когда вы добавляете скрипт, он добавляется на всех устройствах, использующих шаблон. Перед добавлением скрипта требуется настроить подключение VNFM к консоли устройства CPE.

```
---
- hosts: ${target}
  gather_facts: no
  tasks:
    - name: setting up ssh key
      raw: echo ${ssh.key.public} >> /etc/dropbear/authorized_keys
```

Чтобы добавить скрипт:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Скрипты**.

   Отобразятся параметры подключения VNFM к консоли устройства CPE, а также 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 перестает 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** – это значение выбрано по умолчанию.
   - **Shell**.
   - **Expect**.

- **Пользовательский** – использовать собственный интерпретатор в VNFM.

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

8. Если в раскрывающемся списке **Исполнитель скрипта** вы выбрали **Пользовательский**, в поле **Пользовательский интерпретатор** введите путь к интерпретатору.

9. В раскрывающемся списке **Стадия** выберите стадию работы устройства CPE, на которой требуется запустить скрипт:

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

10. При необходимости разрешить повторный запуск скрипта установите флажок **Повторный запуск**. По умолчанию флажок снят.

11. В поле **Скрипт** укажите путь к файлу со скриптом или к файлу-сценарию Ansible playbook.

12. При необходимости в поле **Файл** укажите путь к необходимым для выполнения скрипта дополнительным файлам. Поддерживаемые форматы архивов с файлами: TAR.GZ и ZIP.

13. Нажмите на кнопку **Сохранить**.

Скрипт будет добавлен в шаблон CPE и отобразится в таблице.

Изменение скрипта

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

Чтобы изменить скрипт:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Скрипты**.

   Отобразятся параметры подключения VNFM к консоли устройства CPE, а также таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **Изменить** рядом со скриптом.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по добавлению скрипта.

6. Нажмите на кнопку **Сохранить**.

Просмотр содержимого скрипта

Вы можете просмотреть содержимое скрипта на отдельном устройстве или в шаблоне CPE.

Чтобы просмотреть содержимое скрипта на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Скрипты**.

   Отобразится таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **Просмотреть** рядом со скриптом.

Откроется окно с содержимым скрипта.

Чтобы просмотреть содержимое скрипта в шаблоне CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Скрипты**.

   Отобразятся параметры подключения VNFM к консоли устройства CPE, а также таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **Просмотреть** рядом со скриптом.

Откроется окно с содержимым скрипта.

Удаление скрипта

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

Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Скрипты**.

   Отобразятся параметры подключения VNFM к консоли устройства CPE, а также таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **Удалить** рядом со скриптом.

   Скрипт будет удален и перестанет отображаться в таблице.

5. Нажмите на кнопку **Применить**.

Настройка порядка запуска скриптов

Порядок запуска скриптов используется, когда на устройстве CPE требуется одновременно запустить несколько скриптов, чтобы определить, какой скрипт будет запущен первым.

Например, вы можете добавить два скрипта, каждый из которых автоматически запускается при регистрации устройства. По умолчанию первым запускается скрипт, который был добавлен раньше всех остальных.

Вы можете настроить порядок запуска в шаблоне CPE. Указанный в шаблоне порядок запуска применяется ко всем устройствам, использующим шаблон.

Чтобы настроить порядок запуска скриптов:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Скрипты**.

   Отобразятся параметры подключения VNFM к консоли устройства CPE, а также таблица скриптов, если добавлен хотя бы один скрипт.

4. Настройте порядок выполнения скриптов, используя кнопки **Вниз** и **Вверх** рядом с каждым скриптом. Скрипт, который находится вверху области настройки, будет запущен первым.

5. Нажмите на кнопку **Применить**.

Запуск скриптов вручную

Вы можете запустить скрипт на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Для запуска скрипта вручную используйте следующие инструкции:

- Запуск скрипта на отдельном устройстве CPE.

Чтобы запустить скрипт на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Скрипты**.

   Отобразится таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **Запустить** рядом со скриптом.

5. В открывшемся окне нажмите на кнопку **Запустить**.

- Запуск скрипта на всех устройствах, использующих шаблон CPE.

При запуске скрипта в шаблоне CPE вам нужно выбрать, требуется ли запустить этот скрипт на всех устройствах, использующих шаблон или только на устройствах, которым назначены указанные теги.

Чтобы запустить скрипт на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Скрипты**.

   Отобразятся параметры подключения VNFM к консоли устройства CPE, а также таблица скриптов, если добавлен хотя бы один скрипт.

4. Нажмите на кнопку **Запустить** рядом со скриптом.

5. В открывшемся окне выберите, на каких устройствах требуется запустить скрипт:

   - **Запустить скрипт <имя скрипта> на всех связанных CPE** – запустить скрипт на всех устройствах, использующих шаблон CPE. Это значение выбрано по умолчанию.

   - **Запустить скрипт <имя скрипта> на всех связанных CPE с тегами** – запустить скрипт на устройствах, использующих шаблон CPE, которым назначены определенные теги.

6. Если вы выбрали **Запустить скрипт <имя скрипта> на всех связанных CPE с тегами**, внизу окна укажите теги.

7. Нажмите на кнопку **Запустить**.

При необходимости вы можете запустить все скрипты, добавленные на отдельном устройстве или в шаблоне CPE, одновременно. Для запуска всех скриптов используйте следующие инструкции:

- **Запуск всех скриптов на отдельном устройстве CPE**.

  Чтобы запустить все скрипты на отдельном устройстве CPE:

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

     По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

  2. Нажмите на устройство CPE.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

  3. Выберите вкладку **Скрипты**.

     Отобразится таблица скриптов, если добавлен хотя бы один скрипт.

  4. Вверху области настройки в блоке **Действия** нажмите на кнопку **Запустить скрипты**.

  5. В открывшемся окне нажмите на кнопку **Запустить**.

- **Запуск всех скриптов в шаблоне CPE**.

  При запуске всех добавленных в шаблон CPE скриптов вам нужно выбрать, требуется ли запустить скрипты на всех использующих шаблон устройствах или только на устройствах, которым назначены указанные вами теги.

  Чтобы запустить все скрипты в шаблоне CPE:

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

     Отобразится таблица шаблонов CPE.

  2. Нажмите на шаблон CPE.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

  3. Выберите вкладку **Скрипты**.

     Отобразятся параметры подключения VNFM к консоли устройства CPE, а также таблица скриптов, если добавлен хотя бы один скрипт.

  4. Вверху области настройки в блоке **Действия** нажмите на кнопку **Запустить скрипты**.

  5. В открывшемся окне выберите, на каких устройствах требуется запустить скрипт:

     - **Запустить скрипты на всех связанных CPE** – запустить скрипты на всех устройствах, использующих шаблон CPE. Это значение выбрано по умолчанию.
     - **Запустить скрипты на всех связанных CPE с тегами** – запустить скрипты на устройствах, использующих шаблон CPE, которым назначены определенные теги.

  6. Если вы выбрали **Запустить скрипты на всех связанных CPE с тегами**, внизу окна укажите теги.

  7. Нажмите на кнопку **Запустить**.

Отложенный запуск скриптов

В планировщике создаются отложенные задачи, которые позволяют запустить скрипты на устройствах CPE в указанное время. При создании отложенной задачи необходимо выбрать шаблон CPE, скрипты, а также устройства, на которых требуется запустить скрипты. Вы можете запустить скрипты на всех устройствах, использующих шаблон CPE, либо ограничить количество устройств, выбрав их вручную или указав определенные теги.

Для отложенного запуска скриптов используйте следующие инструкции:

- **Отложенный запуск скриптов на всех устройствах, использующих шаблон CPE**.

  Чтобы создать отложенную задачу по запуску скриптов на всех устройствах, использующих шаблон CPE:

  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 **Запуск скрипта**.

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

  5. В раскрывающемся списке **CPE для запуска скрипта** выберите **Все CPE с выбранным шаблоном**.

  6. В блоке **Шаблон CPE** выберите шаблон CPE.

  7. В блоке **Скрипты** выберите скрипты, которые требуется запустить.

  8. В поле **Дата и время выполнения** введите дату и время выполнения отложенной задачи. По умолчанию указаны дата и время в момент, когда вы начали создавать отложенную задачу.

  9. Нажмите на кнопку **Создать**.

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

- **Отложенный запуск скриптов на устройствах с определенными тегами, использующих шаблон CPE**.

Вы можете сгруппировать устройства CPE, на которых требуется запустить скрипты, назначив им одинаковый тег, после чего приступить к созданию отложенной задачи.

Чтобы создать отложенную задачу по запуску скриптов на устройствах с определенными тегами, использующих шаблон CPE:

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 **Запуск скрипта**.

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

5. В раскрывающемся списке **CPE для запуска скрипта** выберите **Все CPE с выбранным шаблоном и определенными тегами**.

6. В блоке **Шаблон CPE** выберите шаблон CPE.

7. В блоке **Скрипты** выберите скрипты, которые требуется запустить.

8. В поле **Теги** укажите теги, назначенные устройствам CPE, на которых требуется запустить скрипты.

9. В поле **Дата и время выполнения** введите дату и время выполнения отложенной задачи. По умолчанию указаны дата и время в момент, когда вы начали создавать отложенную задачу.

10. Нажмите на кнопку **Создать**.

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

- **Отложенный запуск скриптов на отдельных устройствах, использующих шаблон CPE**

Чтобы создать отложенную задачу по запуску скриптов на отдельных устройствах, использующих шаблон CPE:

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 **Запуск скрипта**.

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

5. В раскрывающемся списке **CPE для запуска скрипта** выберите **Определенные CPE с выбранным шаблоном**.

6. В блоке **Шаблон CPE** выберите шаблон CPE.

7. В блоке **Скрипты** выберите скрипты, которые требуется запустить.

8. В блоке **CPE** выберите устройства CPE, на которых требуется запустить скрипты.

9. В поле **Дата и время выполнения** введите дату и время выполнения отложенной задачи. По умолчанию указаны дата и время в момент, когда вы начали создавать отложенную задачу.

10. Нажмите на кнопку **Создать**.

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

Сетевые интерфейсы

Сетевые интерфейсы – это Linux-интерфейсы для установки соединения с внешними физическими устройствами. Вам нужно назначить IP-адрес каждому сетевому интерфейсу по протоколу DHCP или статически. Поддерживается создание следующих типов сетевых интерфейсов:

- с автоматическим назначением IP-адреса по протоколу DHCP;
- со статическим IPv4-адресом;
- со статическим IPv6-адресом;
- для подключения к беспроводной сети.

Параметры, которые вы можете указать во время создания сетевого интерфейса, зависят от выбранного типа.

Создание сетевого интерфейса

Вы можете создать сетевой интерфейс на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Для создания сетевого интерфейса используйте следующие инструкции:

- Создание сетевого интерфейса с автоматическим назначением IP-адреса по протоколу DHCP на отдельном устройстве CPE.

Чтобы создать сетевой интерфейс и автоматически назначить ему IP-адрес по протоколу DHCP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **+ Сетевой интерфейс**.

5. В открывшемся окне в поле **Псевдоним** введите псевдоним, на который вы сможете сослаться при создании интерфейса SD-WAN. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

   Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

6. В поле **Имя интерфейса** введите имя физического интерфейса на устройстве CPE. Максимальная длина: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких физических интерфейсов введите их имена через пробел.

7. Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

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

9. При необходимости установите следующие флажки:

   - Установите флажок **Включать автоматически**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE.
   - Установите флажок **Назначать IP, маршрут и шлюз**, чтобы автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.
   - Установите флажок **Использовать маршрут по умолчанию**, чтобы использовать на сетевом интерфейсе маршрут по умолчанию, получаемый по протоколу DHCP.

   По умолчанию все флажки установлены

10. При необходимости добавьте DNS-сервер:

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

    b. В отобразившемся поле введите IP-адрес сервера.

Наличие DNS-серверов позволяет сетевым устройствам преобразовывать доменные имена в IP-адреса и таким образом поддерживать зависящие от DNS приложения, такие как браузеры и электронная почта. Вы можете добавить несколько серверов.

11. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет MAC-адрес по умолчанию.

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

13. В поле **Метрика маршрута** введите `100`, если вы создаете первый WAN-интерфейс. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

14. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

15. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- **Создание сетевого интерфейса с автоматическим назначением IP-адреса по протоколу DHCP на всех устройствах, использующих шаблон CPE**.

Чтобы создать сетевой интерфейс и автоматически назначить ему IP-адрес по протоколу DHCP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **+ Сетевой интерфейс**.

5. В открывшемся окне в поле **Псевдоним** введите псевдоним, на который вы сможете сослаться при создании интерфейса SD-WAN. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

   > Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

6. В поле **Имя интерфейса** введите имя физического интерфейса на устройстве CPE. Максимальная длина: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких физических интерфейсов введите их имена через пробел.

7. Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

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

9. При необходимости установите следующие флажки:

   - Установите флажок **Включать автоматически**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE.
   - Установите флажок **Назначать IP, маршрут и шлюз**, чтобы автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.
   - Установите флажок **Использовать маршрут по умолчанию**, чтобы использовать на сетевом интерфейсе маршрут по умолчанию, получаемый по протоколу DHCP.

   По умолчанию все флажки установлены

10. При необходимости добавьте DNS-сервер:

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

    b. В отобразившемся поле введите IP-адрес сервера.

Наличие DNS-серверов позволяет сетевым устройствам преобразовывать доменные имена в IP-адреса и таким образом поддерживать зависящие от DNS приложения, такие как браузеры и электронная почта. Вы можете добавить несколько серверов.

11. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет MAC-адрес по умолчанию.

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

13. В поле **Метрика маршрута** введите `100`, если вы создаете первый WAN-интерфейс. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

14. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

15. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

- Создание сетевого интерфейса со статическим IPv4-адресом на отдельном устройстве CPE.

Чтобы создать сетевой интерфейс и назначить ему статический IPv4-адрес на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **+ Сетевой интерфейс**.

5. В открывшемся окне в поле **Псевдоним** введите псевдоним, на который вы сможете сослаться при создании интерфейса SD-WAN. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

   Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

6. В поле **Имя интерфейса** введите имя физического интерфейса на устройстве CPE. Максимальная длина: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких физических интерфейсов введите их имена через пробел.

7. Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

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

9. При необходимости установите следующие флажки:

   - Установите флажок **Включать автоматически**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE.
   - Установите флажок **Назначать IP, маршрут и шлюз**, чтобы автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.

   По умолчанию все флажки установлены

10. В поле **IPv4-адрес** введите IPv4-адрес сетевого интерфейса. Вы можете ввести несколько адресов через пробел.

11. В поле **IPv4-маска** введите маску IPv4-адреса.

12. В поле **IPv4-шлюз** введите IP-адрес шлюза по умолчанию. Шлюз по умолчанию в сети SD-WAN обеспечивает коммуникацию между устройствами из локальной и внешних сетей.

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

14. При необходимости добавьте DNS-сервер:

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

    b. В отобразившемся поле введите IP-адрес сервера.

    Наличие DNS-серверов позволяет сетевым устройствам преобразовывать доменные имена в IP-адреса и таким образом поддерживать зависящие от DNS приложения, такие как браузеры и электронная почта. Вы можете добавить несколько серверов.

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

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

17. В поле **Метрика маршрута** введите `100`, если вы создаете первый WAN-интерфейс. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

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

    - **Выключен** – это значение выбрано по умолчанию.
    - **Ретранслятор**.
    - **Сервер**.

19. Если в раскрывающемся списке **Тип** вы выбрали **Ретранслятор**, в поле **IP DHCP-сервера** введите IP-адрес сервера.

20. Если в раскрывающемся списке **Тип** вы выбрали **Сервер**, укажите параметры DHCP-сервера:

    a. В поле **Первый IP** введите IP-адрес, с которого требуется начать выдачу адресов клиентам. По умолчанию указано значение `100`.

    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 добавить DHCP-опцию в блоке **DHCP-опции** нажмите на кнопку **+ Добавить** и в отобразившемся поле введите имя опции. Максимальная длина: 250 символов. Вы можете добавить несколько опций.

21. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

22. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание сетевого интерфейса со статическим IPv4-адресом на всех устройствах, использующих шаблон CPE.

Чтобы создать сетевой интерфейс и назначить ему статический IPv4-адрес на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **+ Сетевой интерфейс**.

5. В открывшемся окне в поле **Псевдоним** введите псевдоним, на который вы сможете сослаться при создании интерфейса SD-WAN. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

   Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

6. В поле **Имя интерфейса** введите имя физического интерфейса на устройстве CPE. Максимальная длина: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких физических интерфейсов введите их имена через пробел.

7. Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

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

9. При необходимости установите следующие флажки:

   - Установите флажок **Включать автоматически**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE.
   - Установите флажок **Назначать IP, маршрут и шлюз**, чтобы автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.

   По умолчанию все флажки установлены

10. В поле **IPv4-адрес** введите IPv4-адрес сетевого интерфейса. Вы можете ввести несколько адресов через пробел.

11. В поле **IPv4-маска** введите маску IPv4-адреса.

12. В поле **IPv4-шлюз** введите IP-адрес шлюза по умолчанию. Шлюз по умолчанию в сети SD-WAN обеспечивает коммуникацию между устройствами из локальной и внешних сетей.

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

14. При необходимости добавьте DNS-сервер:

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

    b. В отобразившемся поле введите IP-адрес сервера.

    Наличие DNS-серверов позволяет сетевым устройствам преобразовывать доменные имена в IP-адреса и таким образом поддерживать зависящие от DNS приложения, такие как браузеры и электронная почта. Вы можете добавить несколько серверов.

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

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

17. В поле **Метрика маршрута** введите `100`, если вы создаете первый WAN-интерфейс. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

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

    - **Выключен** – это значение выбрано по умолчанию.
    - **Ретранслятор**.
    - **Сервер**.

19. Если в раскрывающемся списке **Тип** вы выбрали **Ретранслятор**, в поле **IP DHCP-сервера** введите IP-адрес сервера.

20. Если в раскрывающемся списке **Тип** вы выбрали **Сервер**, укажите параметры DHCP-сервера:

    a. В поле **Первый IP** введите IP-адрес, с которого требуется начать выдачу адресов клиентам. По умолчанию указано значение `100`.

    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 добавить DHCP-опцию в блоке **DHCP-опции** нажмите на кнопку **+ Добавить** и в отобразившемся поле введите имя опции. Максимальная длина: 250 символов. Вы можете добавить несколько опций.

21. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

22. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

- Создание сетевого интерфейса со статическим IPv6-адресом на отдельном устройстве CPE.

Чтобы создать сетевой интерфейс и назначить ему статический IPv6-адрес на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **+ Сетевой интерфейс**.

5. В открывшемся окне в поле **Псевдоним** введите псевдоним, на который вы сможете сослаться при создании интерфейса SD-WAN. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

   Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

6. В поле **Имя интерфейса** введите имя физического интерфейса на устройстве CPE. Максимальная длина: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких физических интерфейсов введите их имена через пробел.

7. Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

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

9. При необходимости установите следующие флажки:

   - Установите флажок **Включать автоматически**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE.
   - Установите флажок **Назначать IP, маршрут и шлюз**, чтобы автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.

   По умолчанию оба флажка установлены.

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

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

12. В поле **IPv6-шлюз** введите IP-адрес шлюза по умолчанию. Шлюз по умолчанию в сети SD-WAN обеспечивает коммуникацию между устройствами из локальной и внешних сетей.

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

14. В поле **Суб-префикс DHCPv6** введите длину суб-префикса DHCPv6, который сетевой интерфейс должен назначать клиентам. Максимальная длина: 256 символов.

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

16. При необходимости добавьте IPv6-префиксов:

    a. В блоке **Класс IPv6** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите имя класса. Максимальная длина: 256 символов.

    Сетевой интерфейс принимает добавленные классы префиксов. Вы можете добавить несколько классов.

17. При необходимости добавьте DNS-сервер:

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

    b. В отобразившемся поле введите IP-адрес сервера.

    Наличие DNS-серверов позволяет сетевым устройствам преобразовывать доменные имена в IP-адреса и таким образом поддерживать зависящие от DNS приложения, такие как браузеры и электронная почта. Вы можете добавить несколько серверов.

18. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет MAC-адрес по умолчанию.

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

20. В поле **Метрика маршрута** введите `100`, если вы создаете первый WAN-интерфейс. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

21. В блоке **DHCP-сервер** в раскрывающемся списке **Тип** выберите режим работы используемого DHCP-сервера:

    - **Выключен** – это значение выбрано по умолчанию.
    - **Ретранслятор**.
    - **Сервер**.

22. Если в раскрывающемся списке **Тип** вы выбрали **Ретранслятор**, в поле **IP DHCP-сервера** введите IP-адрес сервера.

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

    a. В поле **Первый IP** введите IP-адрес, с которого требуется начать выдачу адресов клиентам. По умолчанию указано значение `100`.

    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 добавить DHCP-опцию в блоке **DHCP-опции** нажмите на кнопку **+ Добавить** и в отобразившемся поле введите имя опции. Максимальная длина: 250 символов. Вы можете добавить несколько опций.

24. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

25. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание сетевого интерфейса со статическим IPv6-адресом на всех устройствах, использующих шаблон CPE.

Чтобы создать сетевой интерфейс и назначить ему статический IPv6-адрес на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **+ Сетевой интерфейс**.

5. В открывшемся окне в поле **Псевдоним** введите псевдоним, на который вы сможете сослаться при создании интерфейса SD-WAN. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

   Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

6. В поле **Имя интерфейса** введите имя физического интерфейса на устройстве CPE. Максимальная длина: 256 символов. Например, вы можете ввести `eth0`, `eth1`, `eth2`, или `tun0`. Для создания моста из нескольких физических интерфейсов введите их имена через пробел.

7. Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

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

9. При необходимости установите следующие флажки:

   - Установите флажок **Включать автоматически**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE.
   - Установите флажок **Назначать IP, маршрут и шлюз**, чтобы автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.

   По умолчанию оба флажка установлены.

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

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

12. В поле **IPv6-шлюз** введите IP-адрес шлюза по умолчанию. Шлюз по умолчанию в сети SD-WAN обеспечивает коммуникацию между устройствами из локальной и внешних сетей.

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

14. В поле **Суб-префикс DHCPv6** введите длину суб-префикса DHCPv6, который сетевой интерфейс должен назначать клиентам. Максимальная длина: 256 символов.

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

16. При необходимости добавьте IPv6-префиксов:

    a. В блоке **Класс IPv6** нажмите на кнопку **+ Добавить**.

    b. В отобразившемся поле введите имя класса. Максимальная длина: 256 символов.

    Сетевой интерфейс принимает добавленные классы префиксов. Вы можете добавить несколько классов.

17. При необходимости добавьте DNS-сервер:

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

    b. В отобразившемся поле введите IP-адрес сервера.

    Наличие DNS-серверов позволяет сетевым устройствам преобразовывать доменные имена в IP-адреса и таким образом поддерживать зависящие от DNS приложения, такие как браузеры и электронная почта. Вы можете добавить несколько серверов.

18. В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет MAC-адрес по умолчанию.

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

20. В поле **Метрика маршрута** введите `100`, если вы создаете первый WAN-интерфейс. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

21. В блоке **DHCP-сервер** в раскрывающемся списке **Тип** выберите режим работы используемого DHCP-сервера:

    - **Выключен** – это значение выбрано по умолчанию.
    - **Ретранслятор**.
    - **Сервер**.

22. Если в раскрывающемся списке **Тип** вы выбрали **Ретранслятор**, в поле **IP DHCP-сервера** введите IP-адрес сервера.

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

    a. В поле **Первый IP** введите IP-адрес, с которого требуется начать выдачу адресов клиентам. По умолчанию указано значение `100`.

    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 добавить DHCP-опцию в блоке **DHCP-опции** нажмите на кнопку **+ Добавить** и в отобразившемся поле введите имя опции. Максимальная длина: 250 символов. Вы можете добавить несколько опций.

24. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

25. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

- Создание сетевого интерфейса для подключения к беспроводной сети на отдельном устройстве CPE.

Чтобы создать сетевой интерфейс для подключения к беспроводной сети на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **+ Сетевой интерфейс**.

5. В открывшемся окне в поле **Псевдоним** введите псевдоним, на который вы сможете сослаться при создании интерфейса SD-WAN. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

   Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

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

7. В поле **Имя QMI** введите имя модема для подключения к сети. Максимальная длина: 30 символов. Например, вы можете ввести `/dev/cdc-wdm0`.

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

9. В раскрывающемся списке **Тип аутентификации** выберите, какая аутентификация используется на сетевом интерфейсе:

   - **PAP** (Password Authentication Protocol) – клиент отправляет учетные данные в виде текста на сервер аутентификации. Сервер ищет полученные учетные данные в своей базе данных и при успешном совпадении предоставляет клиенту доступ.
   - **CHAP** (Challenge-Handshake Authentication Protocol) – клиент получает от сервера аутентификации случайную строку, объединяет ее с паролем и применяет к ним одностороннюю хеш-функцию, чтобы сгенерировать ответ. Затем сервер получает ответ, производит такие же операции и при успешном совпадении сгенерированных ответов предоставляет клиенту доступ.
   - **PAP и CHAP** – на сетевом интерфейсе используется оба вида аутентификации.
   - **Отсутствует** – на сетевом интерфейсе не используется аутентификация.

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

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

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

    В поле **Задержка** введите время в секундах, которое должно проходить перед началом взаимодействия сетевого интерфейса с модемом. Максимальное значение: 30. Параметр используется, когда загрузка модема занимает слишком много времени.

13. При необходимости добавьте сетевой режим, который требуется использовать на сетевом интерфейсе:

    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**.

    Вы можете добавить несколько режимов.

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, какой IP-стек используется на сетевом интерфейсе:

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

16. Установите флажок **IPv4 через DHCP**, чтобы назначить 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. Установите флажок **Автоподключение**, чтобы автоматически подключать 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, в течение которого сетевой интерфейс должен ожидать 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. В поле **Метрика маршрута** введите `100`, если вы создаете первый WAN-интерфейс. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

23. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

24. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- **Создание сетевого интерфейса для подключения к беспроводной сети на всех устройствах, использующих шаблон CPE**.

Чтобы создать сетевой интерфейс для подключения к беспроводной сети на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **+ Сетевой интерфейс**.

5. В открывшемся окне в поле **Псевдоним** введите псевдоним, на который вы сможете сослаться при создании интерфейса SD-WAN. Максимальная длина: 15 символов. По умолчанию указано значение `eth1`.

   Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

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

7. В поле **Имя QMI** введите имя модема для подключения к сети. Максимальная длина: 30 символов. Например, вы можете ввести `/dev/cdc-wdm0`.

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

9. В раскрывающемся списке **Тип аутентификации** выберите, какая аутентификация используется на сетевом интерфейсе:

   - **PAP** (Password Authentication Protocol) – клиент отправляет учетные данные в виде текста на сервер аутентификации. Сервер ищет полученные учетные данные в своей базе данных и при успешном совпадении предоставляет клиенту доступ.
   - **CHAP** (Challenge-Handshake Authentication Protocol) – клиент получает от сервера аутентификации случайную строку, объединяет ее с паролем и применяет к ним одностороннюю хеш-функцию, чтобы сгенерировать ответ. Затем сервер получает ответ, производит такие же операции и при успешном совпадении сгенерированных ответов предоставляет клиенту доступ.
   - **PAP и CHAP** – на сетевом интерфейсе используется оба вида аутентификации.
   - **Отсутствует** – на сетевом интерфейсе не используется аутентификация.

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

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

указывайте значение для этого параметра.

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

    В поле **Задержка** введите время в секундах, которое должно проходить перед началом взаимодействия сетевого интерфейса с модемом. Максимальное значение: 30. Параметр используется, когда загрузка модема занимает слишком много времени.

13. При необходимости добавьте сетевой режим, который требуется использовать на сетевом интерфейсе:

    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**.

    Вы можете добавить несколько режимов.

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, какой IP-стек используется на сетевом интерфейсе:

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

16. Установите флажок **IPv4 через DHCP**, чтобы назначить 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. Установите флажок **Автоподключение**, чтобы автоматически подключать 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, в течение которого сетевой интерфейс должен ожидать 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. В поле **Метрика маршрута** введите `100`, если вы создаете первый WAN-интерфейс. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

23. Нажмите на кнопку **Создать**.

    Сетевой интерфейс будет создан и отобразится в таблице.

24. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение сетевого интерфейса

Вы можете изменить сетевой интерфейс на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию сетевого интерфейса.

Чтобы изменить сетевой интерфейс на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Установите флажок **Переопределить** рядом с сетевым интерфейсом, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры интерфейса. По умолчанию флажок снят.

5. Нажмите на кнопку **Изменить**.

6. В открывшемся окне измените требуемые параметры сетевого интерфейса.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить сетевой интерфейс на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **Изменить** рядом с сетевым интерфейсом.

5. В открывшемся окне измените требуемые параметры сетевого интерфейса.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Выключение сетевого интерфейса

Вы можете выключить сетевой интерфейс на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE.

Чтобы выключить сетевой интерфейс на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Установите флажок **Переопределить** рядом с сетевым интерфейсом, чтобы игнорировать примененный шаблон CPE и получить возможность выключить интерфейс. По умолчанию флажок снят.

5. Нажмите на кнопку **Выключить** рядом с сетевым интерфейсом.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы выключить сетевой интерфейс на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **Выключить** рядом с сетевым интерфейсом.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление сетевого интерфейса

Вы можете удалить сетевой интерфейс на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. На отдельном устройстве можно удалить только сетевые интерфейсы, которые были созданы локально, а не унаследованы из шаблона. Удаленные сетевые интерфейсы невозможно восстановить.

Чтобы удалить сетевой интерфейс на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **Удалить** рядом с сетевым интерфейсом.

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

Сетевой интерфейс будет удален и перестанет отображаться в таблице.

Чтобы удалить сетевой интерфейс на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры сети**.

   Отобразится таблица сетевых интерфейсов.

4. Нажмите на кнопку **Удалить** рядом с сетевым интерфейсом.

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

Сетевой интерфейс будет удален и перестанет отображаться в таблице.

Настройка подключения устройства CPE к сети SD-WAN

Устройство CPE подключается к сети SD-WAN, чтобы взаимодействовать с плоскостью управления сетью. Вы можете настроить подключение к сети SD-WAN на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE.

Для настройки подключения к сети SD-WAN используйте следующие инструкции:

- **Настройка подключения к сети SD-WAN на отдельном устройстве CPE**.

При настройке подключения к сети SD-WAN на отдельном устройстве CPE вы не можете указать следующие параметры:

- IP-адрес или FQDN оркестратора;
- протокол для подключения устройства к оркестратору;
- номер порта оркестратора;
- протокол для установления OpenFlow-соединения между устройством и контроллером SD-WAN.

Чтобы настроить подключение к сети SD-WAN на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры SD-WAN**.

   По умолчанию выбрана вкладка **Общие параметры**, на которой отображаются параметры подключения к сети SD-WAN.

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 **Авто-перезагрузка** выберите, требуется ли перезагружать устройство CPE при потере связи с контроллером SD-WAN:

   - **Да**.
   - **Нет** – это значение выбрано по умолчанию.

6. Если в раскрывающемся списке **Авто-перезагрузка** вы выбрали **Да**, в поле **Время перезагрузки (сек.)** введите время в секундах, по прошествии которого устройство CPE будет перезагружено при потере связи с контроллером SD-WAN. Диапазон значений: от 60 до 2 073 600.

7. В раскрывающемся списке **Приоритетный интерфейс управления** выберите, каким образом выполняется переключение основной сессии для обеспечения взаимодействия устройства CPE с контроллерами SD-WAN:

   - **Случайно** – новая сессия выбирается случайно. Это значение выбрано по умолчанию.
   - **<интерфейс SD-WAN>** – новой сессией становится сессия, установленная с указанного интерфейса SD-WAN. Если эта сессия недоступна, основная сессия выбирается случайно из оставшихся активных сессий.

8. Если в раскрывающемся списке **Приоритетный интерфейс управления** вы выбрали **<интерфейс SD-WAN>**, при необходимости настройте обратное переключение на предыдущую сессию, когда она восстанавливается:

   a. Установите флажок **Обратное переключение**. По умолчанию флажок снят.

b. В поле **Время** введите время в секундах, по прошествии которого будет переключаться сессия. Диапазон значений: от 0 до 86 400. Если флажок снят, обратное переключение на предыдущую основную сессию не происходит.

9. В поле **Интервал обновления (сек.)** введите интервал времени в секундах для отправки API-запросов от устройства CPE к оркестратору. Эти запросы используются для получения изменений конфигурации. Диапазон значений: от 5 до 300. По умолчанию указано значение `30`.

10. В поле **URL ZTP** введите шаблон веб-адреса для активации устройства CPE с помощью веб-адреса. При вводе шаблона веб-адреса учитывайте следующее:

    - `{config}` – обязательная часть, которая при генерации ссылки из шаблона заменяется на параметры конфигурации для конкретного устройства CPE.
    - Максимальная длина: 128 символов.
    - Обязательно указывать `http` или `https`.

    По умолчанию используется следующий шаблон веб-адреса: `http://192.168.7.1/cgi-bin/luci/config?payload={config}`.

11. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Настройка подключения к сети SD-WAN на всех устройствах, использующих шаблон CPE.

Чтобы настроить подключение к сети SD-WAN на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры SD-WAN**.

   По умолчанию выбрана вкладка **Общие параметры**, на которой отображаются параметры подключения к сети SD-WAN.

4. В поле **IP/FQDN оркестратора** введите IP-адрес или FQDN оркестратора. Максимальная длина: 50 символов.

5. В раскрывающемся списке **Протокол оркестратора** выберите протокол для подключения устройства CPE к оркестратору:

   - **http**;
   - **https** – это значение выбрано по умолчанию.

6. В поле **Порт оркестратора** введите номер порта оркестратора. Диапазон значений: от 0 до 65 535.

7. В раскрывающемся списке **OpenFlow-транспорт** выберите протокол для установления OpenFlow-соединения между устройством CPE и контроллером SD-WAN:

   - **TCP**.
   - **SSL** – это значение выбрано по умолчанию.

8. В раскрывающемся списке **Авто-перезагрузка** выберите, требуется ли перезагружать устройство CPE при потере связи с контроллером SD-WAN:

   - **Да**.
   - **Нет** – это значение выбрано по умолчанию.

9. Если в раскрывающемся списке **Авто-перезагрузка** вы выбрали **Да**, в поле **Время перезагрузки (сек.)** введите время в секундах, по прошествии которого устройство CPE будет перезагружено при потере связи с контроллером SD-WAN. Диапазон значений: от 60 до 2 073 600.

10. В раскрывающемся списке **Приоритетный интерфейс управления** выберите, каким образом выполняется переключение основной сессии для обеспечения взаимодействия устройства CPE с контроллерами SD-WAN:

    - **Случайно** – новая сессия выбирается случайно. Это значение выбрано по умолчанию.
    - **<интерфейс SD-WAN>** – новой сессией становится сессия, установленная с указанного интерфейса SD-WAN. Если эта сессия недоступна, основная сессия выбирается случайно из оставшихся активных сессий.

11. Если в раскрывающемся списке **Приоритетный интерфейс управления** вы выбрали **<интерфейс SD-WAN>**, при необходимости настройте обратное переключение на предыдущую сессию, когда

она восстанавливается:

a. Установите флажок **Обратное переключение**. По умолчанию флажок снят.

b. В поле **Время** введите время в секундах, по прошествии которого будет переключаться сессия. Диапазон значений: от 0 до 86 400. Если флажок снят, обратное переключение на предыдущую основную сессию не происходит.

12. В поле **Интервал обновления (сек.)** введите интервал времени в секундах для отправки API-запросов от устройства CPE к оркестратору. Эти запросы используются для получения изменений конфигурации. Диапазон значений: от 5 до 300. По умолчанию указано значение `30`.

13. В поле **URL ZTP** введите шаблон веб-адреса для активации устройства CPE с помощью веб-адреса. При вводе шаблона веб-адреса учитывайте следующее:

    - `{config}` – обязательная часть, которая при генерации ссылки из шаблона заменяется на параметры конфигурации для конкретного устройства CPE.
    - Максимальная длина: 128 символов.
    - Обязательно указывать `http` или `https`.

    По умолчанию используется следующий шаблон веб-адреса: `http://192.168.7.1/cgi-bin/luci/config?payload={config}`.

14. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Интерфейсы SD-WAN

Интерфейсы SD-WAN (далее также интерфейсы) – это логические интерфейсы для построения топологии сети SD-WAN. Они имеют предопределенные типы и ссылаются на сетевые интерфейсы (сопоставление происходит через псевдоним сетевого интерфейса).

Когда вы создаете интерфейс SD-WAN, для него автоматически создается OpenFlow-интерфейс с указанным вами номером. Kaspersky SD-WAN временно поддерживает создание только WAN-интерфейсов.

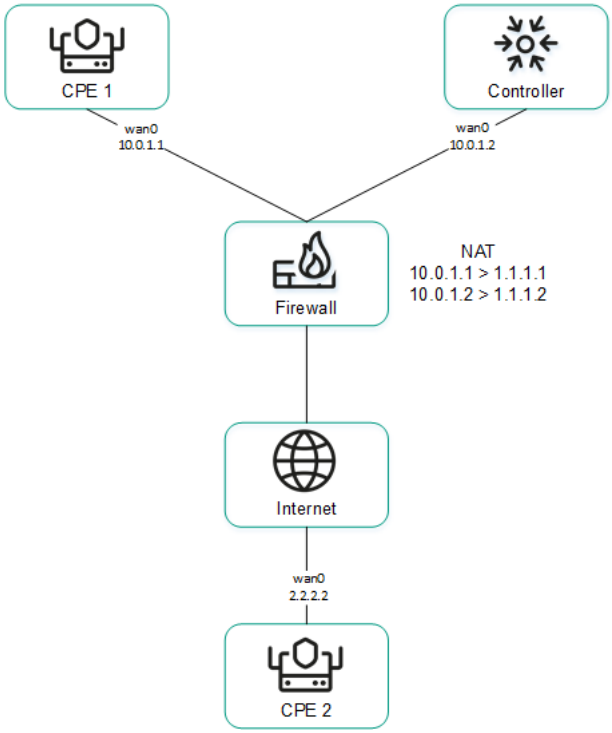
По умолчанию в решении создано два интерфейса SD-WAN, и при необходимости вы можете изменить их параметры.

Передача контроллеру SD-WAN информации о WAN-интерфейсах

Передача контроллеру SD-WAN публичных IP-адресов и UDP-портов WAN-интерфейсов

Для построения GENEVE-туннелей между устройствами CPE контроллеру SD-WAN необходимо получить информацию о публичных IP-адресах WAN-интерфейсов этих устройств. По умолчанию контроллер получает эту информацию с помощью TCP-сессии OpenFlow, которая устанавливается между устройством и контроллером. В этом случае в качестве публичного IP-адреса используется IP-адрес источника.

Если контроллер SD-WAN не в состоянии получить требуемую информацию, вы можете указать IP-адреса и UDP-порты WAN-интерфейсов устройств CPE вручную. На рисунке ниже устройство CPE 1 и контроллер SD-WAN находятся в одной локальной сети и выходят в интернет, используя один сетевой экран, который транслирует IP-адреса. Если при установке сессии между WAN-интерфейсом устройства CPE 1 и публичным IP-адресом контроллера SD-WAN (10.0.1.1 > 1.1.1.2) сетевой 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 WAN-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

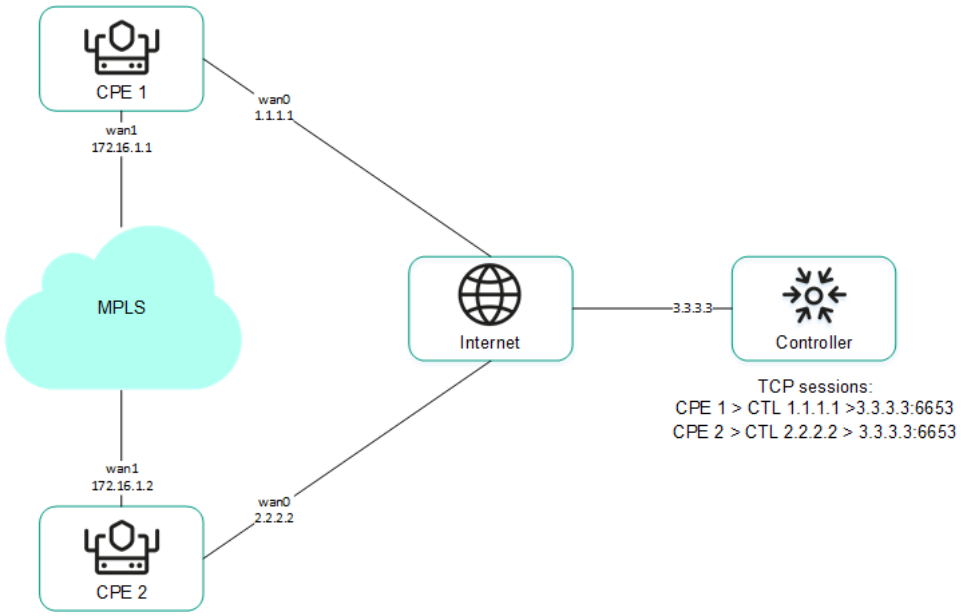
Передача контроллеру SD-WAN IP-адресов WAN-интерфейсов, находящихся в изолированной сети

Некоторые из WAN-интерфейсов устройства CPE могут находиться в изолированной сети без возможности установить TCP-сессию с контроллером SD-WAN, но при этом они могут быть использованы для построения GENEVE-туннелей. В этом случае контроллер не может получить информацию об IP-адресах изолированных WAN-интерфейсов и использовать ее для построения GENEVE-туннелей между устройствами CPE.

На рисунке ниже устройства CPE 1 и 2 имеют по два WAN-интерфейса, но могут установить связь с контроллером SD-WAN 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.

Обратите внимание, что если у одного из устройств CPE выходит из строя канал связи, используемый для взаимодействия с контроллером SD-WAN, все остальные каналы связи также не могут быть использованы, даже если они сохраняют работоспособность, так как контроллер исключает устройство из топологии.

IP-адреса изолированных WAN-интерфейсов можно передать контроллеру SD-WAN через оркестратор.

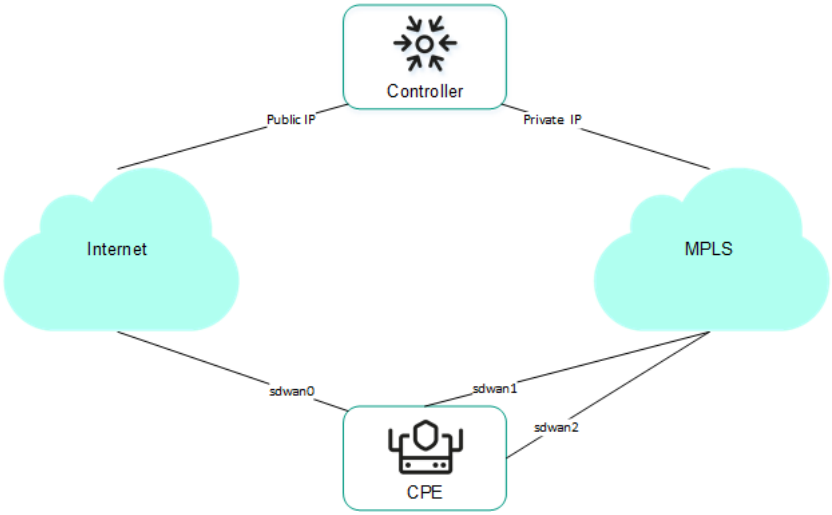


Устройства CPE 1`и 2 связаны друг с другом через MPLS, а также с контроллером SD-WAN через интернет

Вы можете настроить передачу требуемой информации при создании или изменении интерфейса SD-WAN.

Переопределение IP-адреса и порта для подключения интерфейса к контроллеру SD-WAN

Вы можете подключить WAN-интерфейсы к контроллеру SD-WAN, даже если они используют разные типы каналов связи, например интернет и частную MPLS-сеть (см. рисунок ниже). В этом случае вам необходимо вручную переопределить IP-адреса и порты для подключения к контроллеру при создании или изменении интерфейсов.



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 SD-WAN с количеством указанных IP-адресов происходит ошибка и данные остаются прежними.

После переопределения IP-адреса и порта для подключения интерфейса к контроллеру SD-WAN требуется перезагрузить устройство CPE.

Создание интерфейса SD-WAN

Вы можете создать интерфейс SD-WAN на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Интерфейсы SD-WAN создаются поверх сетевых интерфейсов, поэтому сначала требуется создать сетевой интерфейс.

Для создания интерфейса SD-WAN используйте следующие инструкции:

- **Создание интерфейса SD-WAN на отдельном устройстве CPE**.

Чтобы создать интерфейс SD-WAN на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры SD-WAN** → **Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

4. Нажмите на кнопку **+ Интерфейс SD-WAN**.

5. В открывшемся окне в поле **OpenFlow-интерфейс** введите номер OpenFlow-интерфейса, который требуется создать на виртуальном коммутаторе устройства CPE.

6. В поле **Интерфейс (псевдоним)** введите псевдоним сетевого интерфейса, с которым требуется связать OpenFlow-интерфейс.

7. В поле **Максимальная скорость** введите максимальную скорость интерфейса SD-WAN в МБит в секунду. Диапазон значений: от 1 до 100 000. По умолчанию указано значение `1000`.

8. Укажите хоста, доступность которого определяет доступность интерфейса SD-WAN:

   a. В поле **IP для отслеживания** введите IP-адрес хоста.

   b. Нажмите на кнопку **+ Добавить**.

   Вы можете указать несколько хостов.

9. В поле **Надежность** введите количество хостов, которые должны оставаться доступными, чтобы интерфейс SD-WAN считался доступным. По умолчанию указано значение `1`.

   Вам нужно убедиться, что количество хостов в не превышает количество IP-адресов в поле **IP для отслеживания**. В противном случае интерфейс SD-WAN всегда будет считаться недоступным.

10. В поле **Интервал** введите интервал в секундах для проведения тестов интерфейса SD-WAN. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

11. В поле **Количество** введите количество проверок доступности для каждого из указанных хостов в рамках одного теста интерфейса SD-WAN. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

12. В поле **Время** введите время в миллисекундах, в течение которого интерфейс SD-WAN ожидает от хостов эхо-ответа после отправления эхо-запроса. Диапазон значений: от 1 до 100000. По умолчанию указано значение `2000`.

13. В поле **Down** введите интервал в секундах для проведения тестов интерфейса SD-WAN, если он становится недоступным. Диапазон значений: от 1 до 600. По умолчанию указано значение `3`.

14. В поле **Up** введите интервал в секундах для проведения тестов интерфейса SD-WAN, если он снова становится доступным. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

15. В раскрывающемся списке **Мониторинг скорости** выберите, требуется ли проверять ограничение скорости интерфейса SD-WAN оператором мобильной связи:

    - **Да**.
    - **Нет** – это значение выбрано по умолчанию.

16. При необходимости настройте очереди трафика на интерфейсе SD-WAN:

    a. Выберите вкладку **QoS**.

    Отобразится таблица очередей трафика.

    b. В столбце **Изменить ToS** выберите значение Type of Service внешних заголовков пакетов трафика каждой очереди. Вы не можете выбирать эти значения при настройке очередей трафика для LAN-интерфейса.

    c. В столбце **Минимум Скорость, %** укажите минимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN. Сумма значений в столбце не должна превышать 100.

    d. В столбце **Максимум Скорость**, **%** укажите максимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN. Параметр используется для того, чтобы трафик очередей с высоким приоритетом постоянно не вытеснял трафик очередей с низким приоритетом.

    Максимальная скорость интерфейса указывается при настройке подключения устройства CPE к сети SD-WAN на вкладке **Общие параметры** в поле **Максимальная скорость**.

17. При необходимости настройте передачу контроллеру SD-WAN информации об интерфейсе:

    a. Выберите вкладку **NAT и непересекающиеся WAN сети**.

    b. В раскрывающемся списке **Состояние** выберите одно из следующих значений:

    - **Выключено** – контроллеру SD-WAN не требуется передавать информацию об интерфейсе.
    - **NAT/PAT** – интерфейс находится за NAT или PAT и ему требуется назначить публичный IP-адрес и номер UDP-порта, после чего передать их контроллеру SD-WAN.
    - **Непересекающиеся WAN сети** – интерфейс находится в изолированной сети и его IP-адрес требуется передать контроллеру SD-WAN.

    c. Если в раскрывающемся списке **Состояние** вы выбрали **NAT/PAT**, выполните следующие действия:

    1. В поле **Публичный IP-адрес** введите публичный IP-адрес (IPv4) интерфейса.
    2. В поле **Публичный UDP GENEVE порт** введите номер UDP-порта интерфейса. Диапазон значений: от 1 до 65 353.

    d. Если в раскрывающемся списке **Состояние** вы выбрали **Непересекающиеся WAN сети**, в поле **IP-адрес** введите IP-адрес (IPv4) интерфейса. Вам нужно ввести IP-адрес, указанный при создании сетевого интерфейса, поверх которого создается интерфейс SD-WAN.

18. При необходимости переопределите IP-адрес и порт для подключения интерфейса к контроллеру SD-WAN:

    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 вашем экземпляре SD-WAN.

    Вам нужно переопределить IP-адрес для подключения интерфейса к каждому узлу контроллера SD-WAN. В противном случае происходит ошибка и данные остаются прежними.

    d. В поле **Порт** введите номер стартового порта для подключения интерфейса к контроллеру SD-WAN. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**. Диапазон значений: от 1 до 65 535. По умолчанию введено значение `6653`.

    Стартовый порт используется, чтобы определить порты для подключения к контроллеру SD-WAN. Количество определяемых портов зависит от количества WAN-интерфейсов устройства CPE. Например, если вы вводите номер стартового порта `6653`, и устройство имеет четыре WAN-интерфейса, на основании этого порта также определяются порты 6654, 6655 и 6656.

    e. В поле **IP-адрес** введите IP-адрес (IPv4) для подключения интерфейса к контроллеру SD-WAN. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**.

    После переопределения IP-адреса и порта для подключения интерфейса к контроллеру SD-WAN требуется перезагрузить устройство CPE.

19. Нажмите на кнопку **Создать**.

    Интерфейс SD-WAN будет создан и отобразится в таблице.

20. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание интерфейса SD-WAN на всех устройствах, использующих шаблон CPE.

Чтобы создать интерфейс SD-WAN на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

4. Нажмите на кнопку **+ Интерфейс SD-WAN**.

5. В открывшемся окне в поле **OpenFlow-интерфейс** введите номер OpenFlow-интерфейса, который требуется создать на виртуальном коммутаторе устройства CPE.

6. В поле **Интерфейс (псевдоним)** введите псевдоним сетевого интерфейса, с которым требуется связать OpenFlow-интерфейс.

7. В поле **Максимальная скорость** введите максимальную скорость интерфейса SD-WAN в МБит в секунду. Диапазон значений: от 1 до 100 000. По умолчанию указано значение `1000`.

8. Укажите хоста, доступность которого определяет доступность интерфейса SD-WAN:

   a. В поле **IP для отслеживания** введите IP-адрес хоста.

   b. Нажмите на кнопку **+ Добавить**.

   Вы можете указать несколько хостов.

9. В поле **Надежность** введите количество хостов, которые должны оставаться доступными, чтобы интерфейс SD-WAN считался доступным. По умолчанию указано значение `1`.

   Вам нужно убедиться, что количество хостов в не превышает количество IP-адресов в поле **IP для отслеживания**. В противном случае интерфейс SD-WAN всегда будет считаться недоступным.

10. В поле **Интервал** введите интервал в секундах для проведения тестов интерфейса SD-WAN. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

11. В поле **Количество** введите количество проверок доступности для каждого из указанных хостов в рамках одного теста интерфейса SD-WAN. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

12. В поле **Время** введите время в миллисекундах, в течение которого интерфейс SD-WAN ожидает от хостов эхо-ответа после отправления эхо-запроса. Диапазон значений: от 1 до 100000. По умолчанию указано значение `2000`.

13. В поле **Down** введите интервал в секундах для проведения тестов интерфейса SD-WAN, если он становится недоступным. Диапазон значений: от 1 до 600. По умолчанию указано значение `3`.

14. В поле **Up** введите интервал в секундах для проведения тестов интерфейса SD-WAN, если он снова становится доступным. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

15. В раскрывающемся списке **Мониторинг скорости** выберите, требуется ли проверять ограничение скорости интерфейса SD-WAN оператором мобильной связи:

    - **Да**.
    - **Нет** – это значение выбрано по умолчанию.

16. При необходимости настройте очереди трафика на интерфейсе SD-WAN:

    a. Выберите вкладку **QoS**.

    Отобразится таблица очередей трафика.

    b. В столбце **Изменить ToS** выберите значение Type of Service внешних заголовков пакетов трафика каждой очереди. Вы не можете выбирать эти значения при настройке очередей трафика для LAN-интерфейса.

    c. В столбце **Минимум Скорость, %** укажите минимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN. Сумма значений в столбце не должна превышать 100.

    d. В столбце **Максимум Скорость**, **%** укажите максимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN. Параметр используется для того, чтобы трафик очередей с высоким приоритетом постоянно не вытеснял трафик очередей с низким приоритетом.

    Максимальная скорость интерфейса указывается при настройке подключения устройства CPE к сети SD-WAN на вкладке **Общие параметры** в поле **Максимальная скорость**.

17. При необходимости настройте передачу контроллеру SD-WAN информации об интерфейсе:

    a. Выберите вкладку **NAT и непересекающиеся WAN сети**.

    b. В раскрывающемся списке **Состояние** выберите одно из следующих значений:

    - **Выключено** – контроллеру SD-WAN не требуется передавать информацию об интерфейсе.
    - **NAT/PAT** – интерфейс находится за NAT или PAT и ему требуется назначить публичный IP-адрес и номер UDP-порта, после чего передать их контроллеру SD-WAN.
    - **Непересекающиеся WAN сети** – интерфейс находится в изолированной сети и его IP-адрес требуется передать контроллеру SD-WAN.

    c. Если в раскрывающемся списке **Состояние** вы выбрали **NAT/PAT**, выполните следующие действия:

    1. В поле **Публичный IP-адрес** введите публичный IP-адрес (IPv4) интерфейса.
    2. В поле **Публичный UDP GENEVE порт** введите номер UDP-порта интерфейса. Диапазон значений: от 1 до 65 353.

    d. Если в раскрывающемся списке **Состояние** вы выбрали **Непересекающиеся WAN сети**, в поле **IP-адрес** введите IP-адрес (IPv4) интерфейса. Вам нужно ввести IP-адрес, указанный при создании сетевого интерфейса, поверх которого создается интерфейс SD-WAN.

18. При необходимости переопределите IP-адрес и порт для подключения интерфейса к контроллеру SD-WAN:

    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 вашем экземпляре SD-WAN.

    Вам нужно переопределить IP-адрес для подключения интерфейса к каждому узлу контроллера SD-WAN. В противном случае происходит ошибка и данные остаются прежними.

    d. В поле **Порт** введите номер стартового порта для подключения интерфейса к контроллеру SD-WAN. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**. Диапазон значений: от 1 до 65 535. По умолчанию введено значение `6653`.

    Стартовый порт используется, чтобы определить порты для подключения к контроллеру SD-WAN. Количество определяемых портов зависит от количества WAN-интерфейсов устройства CPE. Например, если вы вводите номер стартового порта `6653`, и устройство имеет четыре WAN-интерфейса, на основании этого порта также определяются порты 6654, 6655 и 6656.

    e. В поле **IP-адрес** введите IP-адрес (IPv4) для подключения интерфейса к контроллеру SD-WAN. Количество полей соответствует значению, которое вы выбрали в раскрывающемся списке **Количество контроллеров**.

    После переопределения IP-адреса и порта для подключения интерфейса к контроллеру SD-WAN требуется перезагрузить устройство CPE.

19. Нажмите на кнопку **Создать**.

    Интерфейс SD-WAN будет создан и отобразится в таблице.

20. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение интерфейса SD-WAN

Вы можете изменить интерфейс SD-WAN на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию интерфейса SD-WAN.

Чтобы изменить интерфейс SD-WAN на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

4. Установите флажок **Переопределить** рядом с интерфейсом SD-WAN, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры интерфейса. По умолчанию флажок снят.

5. Нажмите на кнопку **Изменить**.

6. В открывшемся окне измените требуемые параметры интерфейса SD-WAN.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить интерфейс SD-WAN на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

4. Нажмите на кнопку **Изменить** рядом с интерфейсом SD-WAN.

5. В открывшемся окне измените требуемые параметры интерфейса SD-WAN.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Выключение интерфейса SD-WAN

Вы можете выключить интерфейс SD-WAN на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE.

Чтобы выключить интерфейс SD-WAN на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

4. Установите флажок **Переопределить** рядом с интерфейсом SD-WAN, чтобы игнорировать примененный шаблон CPE и получить возможность выключить интерфейс. По умолчанию флажок снят.

5. Нажмите на кнопку **Выключить**.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы выключить интерфейс SD-WAN на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

4. Нажмите на кнопку **Выключить** рядом с интерфейсом SD-WAN.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление интерфейса SD-WAN

Вы можете удалить интерфейс SD-WAN на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. На отдельном устройстве можно удалить только интерфейсы SD-WAN, которые были созданы локально, а не унаследованы из шаблона. Удаленные интерфейсы SD-WAN невозможно восстановить.

Чтобы удалить сетевой интерфейс на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

4. Нажмите на кнопку **Удалить** рядом с интерфейсом SD-WAN.

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

Интерфейс SD-WAN будет удален и перестанет отображаться в таблице.

Чтобы удалить интерфейс SD-WAN на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры SD-WAN → Интерфейсы**.

   Отобразится таблица интерфейсов SD-WAN.

4. Нажмите на кнопку **Удалить** рядом с интерфейсом SD-WAN.

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

Интерфейс SD-WAN будет удален и перестанет отображаться в таблице.

OpenFlow-интерфейсы

OpenFlow-интерфейсы – это интерфейсы наложенной SDN-сети, которые создаются автоматически одновременно с интерфейсами SD-WAN. Контроллер SD-WAN использует OpenFlow-интерфейсы, чтобы управлять трафиком сети. Поверх OpenFlow-интерфейсов создаются сервисные интерфейсы и UNI.

Вы можете объединить OpenFlow-интерфейсы в группы и использовать их при создании транспортных сервисов M2M и P2M. Когда вы добавляете группу OpenFlow-интерфейсов в транспортный сервис, поверх каждого интерфейса в группе автоматически создается сервисный интерфейс, который в свою очередь используется транспортным сервисом.

Использование групп OpenFlow-интерфейсов избавляет вас от необходимости вручную создавать сервисные интерфейсы и добавлять их в транспортные сервисы.

Создание группы OpenFlow-интерфейсов

Чтобы создать группу OpenFlow-интерфейсов:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **OpenFlow-группы**.

   Отобразится таблица групп OpenFlow-интерфейсов.

4. Вверху страницы нажмите на кнопку **+ OpenFlow-группа**.

5. В открывшемся окне в поле **Имя** введите имя группы OpenFlow-интерфейсов.

6. В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-интерфейс, который требуется добавить в группу.

7. Нажмите на кнопку **Создать**.

Группа OpenFlow-интерфейсов будет создана и отобразится в таблице.

Изменение группы OpenFlow-интерфейсов

Чтобы изменить группу OpenFlow-интерфейсов:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **OpenFlow-группы**.

   Отобразится таблица групп OpenFlow-интерфейсов.

4. Нажмите на кнопку **Управление** рядом с группой OpenFlow-интерфейсов и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию группы OpenFlow-интерфейсов.

6. Нажмите на кнопку **Сохранить**.

Удаление группы OpenFlow-интерфейсов

Удаленные группы OpenFlow-интерфейсов невозможно восстановить.

Чтобы удалить группу OpenFlow-интерфейсов:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **OpenFlow-группы**.

   Отобразится таблица групп OpenFlow-интерфейсов.

4. Нажмите на кнопку **Управление** рядом с группой OpenFlow-интерфейсов и в раскрывающемся списке выберите **Удалить**.

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

Группа OpenFlow-интерфейсов будет удалена и перестанет отображаться в таблице.

Сервисные интерфейсы и UNI

Сервисные интерфейсы и UNI – это интерфейсы для подключения устройств к транспортным и сетевым сервисам. Эти интерфейсы создаются поверх любых OpenFlow-интерфейсов за исключением тех, которые соответствуют WAN-интерфейсам SD-WAN.

Поверх сервисных интерфейсов в свою очередь можно создать *ACL-интерфейсы*, которые обеспечивают фильтрацию трафика между транспортными сервисами на основании указанных вами ограничений.

Вы можете создать все необходимые UNI в одном шаблоне UNI, после чего применять его устройству CPE при создании и регистрации этого устройства. В этом случае все UNI из шаблона автоматически создаются на устройстве CPE.

Разница между UNI (user network interface) и сервисными интерфейсами заключается в том, что UNI используются при создании сетевых сервисов, а сервисные интерфейсы – при создании транспортных сервисов. Кроме того, сервисные интерфейсы невозможно добавить в графический конструктор, в котором осуществляется построение топологии сетевого сервиса, а также назначить тенантам.

Обратите внимание, что при создании UNI для него автоматически создается соответствующий сервисный интерфейс, однако для сервисных интерфейсов не создается UNI.

Создание сервисного интерфейса

Чтобы создать сервисный интерфейс:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Сервисные интерфейсы**.

   Отобразится таблица сервисных и ACL-интерфейсов.

4. Вверху страницы в раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-интерфейс.

5. Нажмите на кнопку **Создать сервисный интерфейс**.

6. В открывшемся окне в раскрывающемся списке **Тип** выберите тип инкапсуляции на сервисном интерфейсе:

   - **Access** – это значение выбрано по умолчанию.
   - **VLAN**.
   - **Q-in-Q**.
   - **ACL** – используется для создания ACL-интерфейса.

7. Если в раскрывающемся списке **Тип** вы выбрали **VLAN**, в поле **VLAN ID** введите внешнюю метку VLAN. Диапазон значений: от 1 до 4094.

8. Если в раскрывающемся списке **Тип** 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.

9. При необходимости в поле **Описание** введите краткое описание сервисного интерфейса.

10. Нажмите на кнопку **Создать**.

Сервисный интерфейс будет создан и отобразится в таблице.

Создание ACL-интерфейса

ACL-интерфейс создается поверх сервисного интерфейса и фильтрует трафик, передающийся между транспортными сервисами. Перед созданием ACL-интерфейса требуется выполнить следующие действия:

- создать сервисный интерфейс;
- создать фильтр трафика.

Чтобы создать ACL-интерфейс:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Сервисные интерфейсы**.

   Отобразится таблица сервисных и ACL-интерфейсов.

4. Вверху страницы в раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-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, поверх которого требуется создать ACL-интерфейс.

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 используемый в ACL-интерфейсе фильтр отбрасывает трафик, он направляется во второй по порядку ACL-интерфейс и так далее.

   Диапазон значений: от 1 до 4. Поверх одного сервисного интерфейса невозможно создать два ACL-интерфейса с одинаковым порядковым номером.

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 компоненты решения используют сервисный интерфейс или ACL-интерфейс.

Чтобы просмотреть использование сервисного интерфейса или ACL-интерфейса:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Сервисные интерфейсы**.

   Отобразится таблица сервисных и ACL-интерфейсов.

4. Нажмите на кнопку **Управление** рядом с интерфейсом и в раскрывающемся списке выберите **Показать использование**.

Откроется окно, в котором отображается таблица компонентов решения, использующих интерфейс.

Удаление сервисного интерфейса и ACL-интерфейса

Вы не можете удалить сервисный интерфейс или ACL-интерфейс, который используется компонентом решения, например транспортными сервисом. Удаленные интерфейсы невозможно восстановить.

Чтобы удалить сервисный интерфейс или ACL-интерфейс:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **Сервисные интерфейсы**.

   Отобразится таблица сервисных и ACL-интерфейсов.

4. Нажмите на кнопку **Управление** рядом с интерфейсом и в раскрывающемся списке выберите **Удалить**.

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

Интерфейс будет удален и перестанет отображаться в таблице.

Создание шаблона UNI

Шаблон UNI используется для централизованного создания UNI на устройствах CPE. После создания шаблона в нем создаются необходимые UNI. Затем шаблон применяется к устройству при создании или регистрации этого устройства. Все UNI, созданные в шаблоне, автоматически создаются на устройстве.

Чтобы создать шаблон UNI:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Вверху страницы нажмите на кнопку **+ Шаблон UNI**.

3. В открывшемся окне введите имя шаблона и нажмите на кнопку **Создать**.

Откроется подраздел **Шаблоны UNI**, в котором отображается таблица шаблонов UNI. Шаблон будет создан и отобразится в таблице.

В шаблоне UNI необходимо создать UNI.

Создание UNI в шаблоне

После создания шаблона в нем необходимо создать UNI. Когда вы применяете шаблон к устройству CPE, все созданные в шаблоне UNI автоматически создаются на этом устройстве. Перед созданием UNI в шаблоне требуется создать шаблон UNI.

Чтобы создать UNI в шаблоне:

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

   Отобразится таблица шаблонов UNI.

2. Нажмите на шаблон UNI.

Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **UNI**.

   Отобразится таблица UNI.

4. Нажмите на кнопку **+ UNI**.

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

6. В поле **OpenFlow-интерфейс** введите номер OpenFlow-интерфейса, поверх которого требуется создать UNI.

7. В раскрывающемся списке **OpenFlow-интерфейс** выберите тип инкапсуляции на UNI:

   - **Access** – это значение выбрано по умолчанию.
   - **VLAN**.
   - **Q-in-Q**.

8. Если в раскрывающемся списке **Инкапсуляция** вы выбрали **VLAN**, в поле **VLAN ID** введите внешнюю метку VLAN. Диапазон значений: от 1 до 4094.

9. 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.

10. Нажмите на кнопку **Создать**.

    UNI будет создан в шаблоне и отобразится в таблице.

11. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона UNI.

Изменение UNI в шаблоне

Чтобы изменить UNI в шаблоне:

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

   Отобразится таблица шаблонов UNI.

2. Нажмите на шаблон UNI.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **UNI**.

   Отобразится таблица UNI.

4. Нажмите на кнопку **Изменить** рядом с UNI.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию UNI в шаблоне.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона UNI.

Удаление UNI в шаблоне

Удаленные в шаблоне UNI невозможно восстановить.

Чтобы удалить UNI в шаблоне:

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

   Отобразится таблица шаблонов UNI.

2. Нажмите на шаблон UNI.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **UNI**.

   Отобразится таблица UNI.

4. Нажмите на кнопку **Удалить** рядом с UNI.

   UNI будет удален в шаблоне и перестанет отображаться в таблице.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона UNI.

Удаление шаблона UNI

Удаленные шаблоны UNI невозможно восстановить.

Чтобы удалить шаблон UNI:

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

   Отобразится таблица шаблонов UNI.

2. Нажмите на шаблон UNI.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Вверху 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.

Создание UNI

Вы можете создать UNI на отдельном устройстве CPE. Перед созданием UNI требуется выполнить следующие действия:

- активировать устройство CPE;
- создать QoS-правило.

Чтобы создать UNI на устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **UNI**.

   Отобразится таблица UNI.

4. Нажмите на кнопку **+ UNI**.

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

6. В раскрывающемся списке **Порт** выберите OpenFlow-интерфейс, поверх которого требуется создать UNI.

7. В раскрывающемся списке **Инкапсуляция** выберите тип инкапсуляции на UNI:

   - **Access** – это значение выбрано по умолчанию.
   - **VLAN**.
   - **Q-in-Q**.

8. Если в раскрывающемся списке **Инкапсуляция** вы выбрали **VLAN**, в поле **VLAN ID** введите внешнюю метку VLAN. Диапазон значений: от 1 до 4094.

9. 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.

10. В раскрывающемся списке **QoS** выберите ранее созданное QoS-правило для UNI.

11. Нажмите на кнопку **Создать**.

    UNI будет создан и отобразится в таблице.

12. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Изменение UNI

Вы можете изменить UNI на отдельном устройстве CPE.

Чтобы изменить UNI:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **UNI**.

   Отобразится таблица UNI.

4. Нажмите на кнопку **Изменить** рядом с UNI.

5. В открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию UNI.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Удаление UNI

Вы можете удалить UNI на отдельном устройстве CPE. Удаленные UNI невозможно восстановить.

Чтобы удалить UNI:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **UNI**.

   Отобразится таблица UNI.

4. Нажмите на кнопку **Удалить** рядом с UNI.

   UNI будет удален и перестанет отображаться в таблице.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Фильтрация маршрутов

Фильтрация маршрутов позволяет управлять передачей сетевых маршрутов на основании указанных вами критериев. Эта функциональность необходима для обеспечения оптимальной производительности и безопасности сети, а также для предотвращения петель маршрутизации.

Вы можете использовать фильтрацию маршрутов, чтобы разрешить или запретить анонсирование определенных маршрутов между устройствами CPE и сторонними сетевыми устройствами, а также между отдельными автономными системами. В Kaspersky SD-WAN для фильтрации маршрутов используются списки управления доступом (англ. Access Control Lists, ACL), списки префиксов (англ. prefix lists) и карты маршрутизации (англ. route maps).

Списки управления доступом

Список управления доступом – это набор правил фильтрации маршрутной информации на устройстве CPE на основании IP-адресов и префиксов сетей, которым принадлежат маршруты.

Правила в списке управления доступом могут разрешать или запрещать анонсирование маршрутов, принадлежащих определенной сети. Каждое правило имеет порядковый номер. Устройство CPE будет сравнивать информацию о сети, которой принадлежит маршрут, с условиями правил в используемом списке управления доступом, начиная с правила, имеющего наименьший порядковый номер.

Списки префиксов

Список префиксов является расширенной версией списка управления доступом. Отличием списка префиксов является то, что он может содержать правила, которые фильтруют маршруты на основании IP-адресов и диапазонов префиксов (а не отдельных префиксов) сетей.

Карты маршрутизации

В то время как список управления доступом и список префиксов всегда применяются к анонсируемым маршрутам, *карта маршрутизации* применяется к маршрутам только при выполнении указанных вами условий и может изменять атрибуты маршрутов.

Если ни одно из правил в списке управления доступом, списке префиксов или карте маршрутизации не может быть применено к маршруту, этот маршрут отбрасывается.

Создание списка управления доступом (ACL)

Вы можете создать список управления доступом на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Для создания списка управления доступом используйте следующие инструкции:

- Создание списка управления доступом на отдельном устройстве CPE.

Чтобы создать список управления доступом на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Фильтры маршрутов**.

   По умолчанию выбрана вкладка **Списки управления доступом**, на которой отображается таблица списков управления доступом.

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 **+ Список управления доступом**.

6. В открывшемся окне в поле **Имя** введите имя списка управления доступом. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

7. Нажмите на кнопку **+ Добавить правило**, чтобы добавить правило в список управления доступом. Вы можете добавить несколько правил.

8. В поле **Порядок** введите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.

9. В раскрывающемся списке **Сеть** выберите тип правила:

   - **Любая сеть** – правило, разрешающее или запрещающее анонсирование любых сетей.
   - **IP/маска** – правило, разрешающее или запрещающее анонсирование определенной сети. Это значение выбрано по умолчанию.

10. Если в раскрывающемся списке **Сеть** вы выбрали **IP/маска**, в отобразившемся поле введите IP-адрес и префикс сети.

11. В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:

    - **Разрешить** – разрешить анонсирование маршрутов. Это значение выбрано по умолчанию.
    - **Отклонить** – запретить анонсирование маршрутов.

12. Нажмите на кнопку **Создать**.

    Список управления доступом будет создан и отобразится в таблице.

13. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание списка управления доступом на всех устройствах, использующих шаблон CPE

Чтобы создать список управления доступом на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов**.

   По умолчанию выбрана вкладка **Списки управления доступом**, на которой отображается таблица списков управления доступом.

4. Нажмите на кнопку **+ Список управления доступом**.

5. В открывшемся окне в поле **Имя** введите имя списка управления доступом. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

6. Нажмите на кнопку **+ Добавить правило**, чтобы добавить правило в список управления доступом. Вы можете добавить несколько правил.

7. В поле **Порядок** введите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.

8. В раскрывающемся списке **Сеть** выберите тип правила:

   - **Любая сеть** – правило, разрешающее или запрещающее анонсирование любых сетей.
   - **IP/маска** – правило, разрешающее или запрещающее анонсирование определенной сети. Это значение выбрано по умолчанию.

9. Если в раскрывающемся списке **Сеть** вы выбрали **IP/маска**, в отобразившемся поле введите IP-адрес и префикс сети.

10. В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:

    - **Разрешить** – разрешить анонсирование маршрутов. Это значение выбрано по умолчанию.
    - **Отклонить** – запретить анонсирование маршрутов.

11. Нажмите на кнопку **Создать**.

    Список управления доступом будет создан и отобразится в таблице.

12. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение списка управления доступом

Вы можете изменить список управления доступом на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции со созданию списка управления доступом.

Чтобы изменить список управления доступом на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов**.

   По умолчанию выбрана вкладка **Списки управления доступом**, на которой отображается таблица списков управления доступом.

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 **Изменить** рядом со списком управления доступом.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить список управления доступом на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов**.

   По умолчанию выбрана вкладка **Списки управления доступом**, на которой отображается таблица списков управления доступом.

4. Нажмите на кнопку **Изменить** рядом со списком управления доступом.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление списка управления доступом

Вы можете удалить список управления доступом на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные списки управления доступом невозможно восстановить.

Чтобы удалить список управления доступом на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов**.

   По умолчанию выбрана вкладка **Списки управления доступом**, на которой отображается таблица списков управления доступом.

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 **Удалить** рядом со списком управления доступом.

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

   Список управления доступом будет удален и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить список управления доступом на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов**.

   По умолчанию выбрана вкладка **Списки управления доступом**, на которой отображается таблица списков управления доступом.

4. Нажмите на кнопку **Удалить** рядом со списком управления доступом.

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

   Список управления доступом будет удален и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание списка префиксов (prefix list)

Вы можете создать список префиксов на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Для создания списка префиксов используйте следующие инструкции:

- Создание списка префиксов на отдельном устройстве CPE.

Чтобы создать список префиксов на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

3. Выберите вкладку **Фильтры маршрутов** → **Списки префиксов**.

   Отобразится таблица списков префиксов.

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 **+ Список префиксов**.

6. В открывшемся окне в поле **Имя** введите имя списка префиксов. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

7. Нажмите на кнопку **+ Добавить правило**, чтобы добавить правило в список префиксов. Вы можете добавить несколько правил.

8. В поле **Порядок** введите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.

9. В раскрывающемся списке **Сеть** выберите тип правила:

   - **Любая сеть** – правило, разрешающее или запрещающее анонсирование любых сетей.
   - **IP/маска** – правило, разрешающее или запрещающее анонсирование определенной сети. Это значение выбрано по умолчанию.

10. Если в раскрывающемся списке **Сеть** вы выбрали **IP/маска**, в отобразившемся поле введите IP-адрес и префикс сети.

11. В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:

    - **Разрешить** – разрешить анонсирование маршрутов. Это значение выбрано по умолчанию.
    - **Отклонить** – запретить анонсирование маршрутов.

12. В полях **Greater or equal** и **Less or equal** введите начальное и конечное значение диапазона префиксов. Диапазон значений в каждом поле: от 0 до 32.

13. Нажмите на кнопку **Создать**.

    Список префиксов будет создан и отобразится в таблице.

14. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание списка префиксов на всех устройствах, использующих шаблон CPE.

Чтобы создать список префиксов на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

3. Выберите вкладку **Фильтры маршрутов → Списки префиксов**.

   Отобразится таблица списков префиксов.

4. Нажмите на кнопку **+ Список префиксов**.

5. В открывшемся окне в поле **Имя** введите имя списка префиксов. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

6. Нажмите на кнопку **+ Добавить правило**, чтобы добавить правило в список префиксов. Вы можете добавить несколько правил.

7. В поле **Порядок** введите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.

8. В раскрывающемся списке **Сеть** выберите тип правила:

   - **Любая сеть** – правило, разрешающее или запрещающее анонсирование любых сетей.
   - **IP/маска** – правило, разрешающее или запрещающее анонсирование определенной сети. Это значение выбрано по умолчанию.

9. Если в раскрывающемся списке **Сеть** вы выбрали **IP/маска**, в отобразившемся поле введите IP-адрес и префикс сети.

10. В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:

    - **Разрешить** – разрешить анонсирование маршрутов. Это значение выбрано по умолчанию.
    - **Отклонить** – запретить анонсирование маршрутов.

11. В полях **Greater or equal** и **Less or equal** введите начальное и конечное значение диапазона префиксов. Диапазон значений в каждом поле: от 0 до 32.

12. Нажмите на кнопку **Создать**.

    Список префиксов будет создан и отобразится в таблице.

13. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение списка префиксов

Вы можете изменить список префиксов на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию списка префиксов.

Чтобы изменить список префиксов на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов** → **Списки префиксов**.

   Отобразится таблица списков префиксов.

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 **Изменить** рядом со списком префиксов.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить список префиксов на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов** → **Списки префиксов**.

   Отобразится таблица списков префиксов.

4. Нажмите на кнопку **Изменить** рядом со списком префиксов.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление списка префиксов

Вы можете удалить список префиксов на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные списки префиксов невозможно восстановить.

Чтобы удалить список префиксов на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Фильтры маршрутов** → **Списки префиксов**.

   Отобразится таблица списков префиксов.

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 **Удалить** рядом со списком префиксов.

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

   Список префиксов будет удален и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить список префиксов на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Фильтры маршрутов** → **Списки префиксов**.

   Отобразится таблица списков префиксов.

4. Нажмите на кнопку **Удалить** рядом со списком префиксов.

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

   Список префиксов будет удален и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание карты маршрутизации (route map)

Вы можете создать карту маршрутизации на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Для создания карты маршрутизации используйте следующие инструкции:

- Создание карты маршрутизации на отдельном устройстве CPE.

Чтобы создать карту маршрутизации на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации**.

   Отобразится таблица карт маршрутизации.

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 **+ Карта маршрутизации**.

6. В открывшемся окне в поле **Имя** введите имя карты маршрутизации. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

7. Нажмите на кнопку **+ Добавить правило**, чтобы добавить правило в карту маршрутизации. Вы можете добавить несколько правил.

8. В поле **Порядок** введите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.

9. В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:

   - **Разрешить** – разрешить анонсирование маршрутов. Это значение выбрано по умолчанию.
   - **Отклонить** – запретить анонсирование маршрутов.

10. В раскрывающемся списке **Условие** выберите условие, выполнение которого необходимо для применения правила к маршруту:

    - **Отсутствует** – применять правило ко всем маршрутам. Вы не можете изменять значения атрибутов с помощью этого правила. Это значение выбрано по умолчанию.
    - **Prefix-List** – применять правило к маршрутам, соответствующим выбранному вами списку префиксов.
    - **Community** – применять правило к маршрутам, имеющим атрибут community с указанным вами значением.
    - **Extcommunity** – применять правило к маршрутам, имеющим атрибут extended community с указанным вами значением.

11. Если в раскрывающемся списке **Условие** вы выбрали **Prefix-List**, в раскрывающемся списке **Список префиксов** выберите список префиксов.

12. Если в раскрывающемся списке **Условие** вы выбрали **Community** или **Extcommunity**, в поле **Значение** введите значение атрибута.

13. В раскрывающемся списке **Изменить атрибут** выберите атрибут, значение которого требуется изменить при применении правила к маршруту:

    - **Отсутствует** – не изменять значения атрибутов. Это значение выбрано по умолчанию.
    - **IP next-hop** – изменить значение атрибута next hop. В качестве нового значения требуется ввести IP-адрес.
    - **Local preference** – изменить значение атрибута local preference. Диапазон значений: от 0 до 4 294 967 295.
    - **Metric** – изменить значение атрибута MED. Диапазон значений: от 0 до 4 294 967 295.
    - **Community** – изменить значение атрибута community.
    - **Extcommunity** – изменить значение атрибута extended community.
    - **VPNv4 next-hop** – изменить значение атрибута next hop для VPNv4-маршрутов. В качестве нового значения требуется ввести IPv4-адрес.
    - **AS path preprend** – добавить номер автономной системы в атрибут as path. Вы можете указать несколько номеров через пробел.

14. В поле **Новое значение** введите значение, которое требуется присвоить атрибуту. В зависимости от атрибута, выбранного в раскрывающемся списке **Изменить атрибут**, вы можете вводить цифры или символы.

15. Нажмите на кнопку **Создать**.

    Карта маршрутизации будет создана и отобразится в таблице.

16. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание карты маршрутизации на всех устройствах, использующих шаблон CPE.

Чтобы создать карту маршрутизации на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов → Карты маршрутизации**.

   Отобразится таблица карт маршрутизации.

4. Нажмите на кнопку **+ Карта маршрутизации**.

5. В открывшемся окне в поле **Имя** введите имя карты маршрутизации. Максимальная длина: 50 символов. Не используйте пробелы в этом поле.

6. Нажмите на кнопку **+ Добавить правило**, чтобы добавить правило в карту маршрутизации. Вы можете добавить несколько правил.

7. В поле **Порядок** введите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.

8. В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:

   - **Разрешить** – разрешить анонсирование маршрутов. Это значение выбрано по умолчанию.
   - **Отклонить** – запретить анонсирование маршрутов.

9. В раскрывающемся списке **Условие** выберите условие, выполнение которого необходимо для применения правила к маршруту:

   - **Отсутствует** – применять правило ко всем маршрутам. Вы не можете изменять значения атрибутов с помощью этого правила. Это значение выбрано по умолчанию.
   - **Prefix-List** – применять правило к маршрутам, соответствующим выбранному вами списку префиксов.
   - **Community** – применять правило к маршрутам, имеющим атрибут community с указанным вами значением.
   - **Extcommunity** – применять правило к маршрутам, имеющим атрибут extended community с указанным вами значением.

10. Если в раскрывающемся списке **Условие** вы выбрали **Prefix-List**, в раскрывающемся списке **Список префиксов** выберите список префиксов.

11. Если в раскрывающемся списке **Условие** вы выбрали **Community** или **Extcommunity**, в поле **Значение** введите значение атрибута.

12. В раскрывающемся списке **Изменить атрибут** выберите атрибут, значение которого требуется изменить при применении правила к маршруту:

    - **Отсутствует** – не изменять значения атрибутов. Это значение выбрано по умолчанию.

- **IP next-hop** – изменить значение атрибута next hop. В качестве нового значения требуется ввести IP-адрес.
- **Local preference** – изменить значение атрибута local preference. Диапазон значений: от 0 до 4 294 967 295.
- **Metric** – изменить значение атрибута MED. Диапазон значений: от 0 до 4 294 967 295.
- **Community** – изменить значение атрибута community.
- **Extcommunity** – изменить значение атрибута extended community.
- **VPNv4 next-hop** – изменить значение атрибута next hop для VPNv4-маршрутов. В качестве нового значения требуется ввести IPv4-адрес.
- **AS path preprend** – добавить номер автономной системы в атрибут as path. Вы можете указать несколько номеров через пробел.

13. В поле **Новое значение** введите значение, которое требуется присвоить атрибуту. В зависимости от атрибута, выбранного в раскрывающемся списке **Изменить атрибут**, вы можете вводить цифры или символы.
14. Нажмите на кнопку **Создать**.

    Карта маршрутизации будет создана и отобразится в таблице.
15. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение карты маршрутизации

Вы можете изменить карту маршрутизации на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию карты маршрутизации.

Чтобы изменить карту маршрутизации на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.
2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.
3. Выберите вкладку **Фильтры маршрутов** → **Карты маршрутизации**.

   Отобразится таблица карт маршрутизации.
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 **Изменить** рядом с картой маршрутизации.
6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить карту маршрутизации на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов → Карты маршрутизации**.

   Отобразится таблица карт маршрутизации.

4. Нажмите на кнопку **Изменить** рядом с картой маршрутизации.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление карты маршрутизации

Вы можете удалить карту маршрутизации на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные карты маршрутизации невозможно восстановить.

Чтобы удалить карту маршрутизации на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов → Карты маршрутизации**.

   Отобразится таблица карт маршрутизации.

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 **Удалить** рядом с картой маршрутизации.

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

   Карта маршрутизации будет удалена и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить карту маршрутизации на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Фильтры маршрутов → Карты маршрутизации**.

   Отобразится таблица карт маршрутизации.

4. Нажмите на кнопку **Удалить** рядом с картой маршрутизации.

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

   Карта маршрутизации будет удалена и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

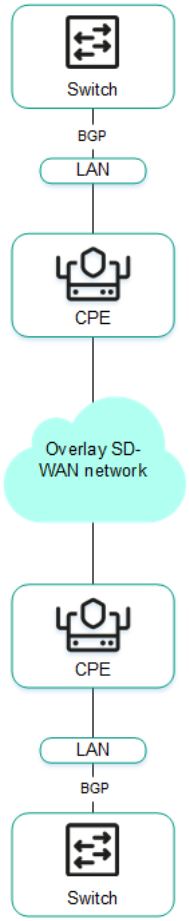
Протокол динамической маршрутизации BGP

Kaspersky SD-WAN поддерживает использование протокола динамической маршрутизации BGP (Border Gateway Protocol) для обмена маршрутной информацией между подключенными к вашей сети SD-WAN устройствами CPE, а также со сторонними сетевыми устройствами. Вы можете устанавливать как внутренние сессии iBGP (internal BGP), так и внешние сессии eBGP (external BGP).

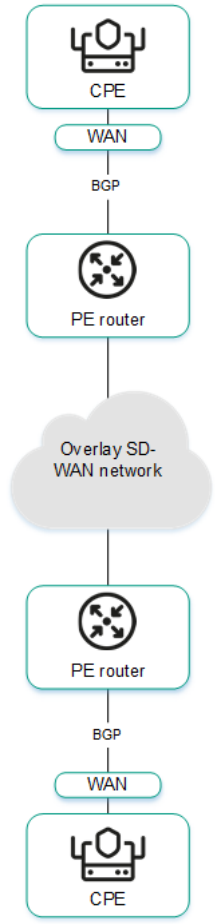
Также поддерживается установка динамических TCP-сессий с группами BGP-соседей (англ. BGP peer groups). Установив динамическую TCP-сессию, вам не нужно создавать отдельных BGP-соседей (англ. BGP peers).

На рисунках ниже представлены примеры использования протокола динамической маршрутизации BGP в решении:

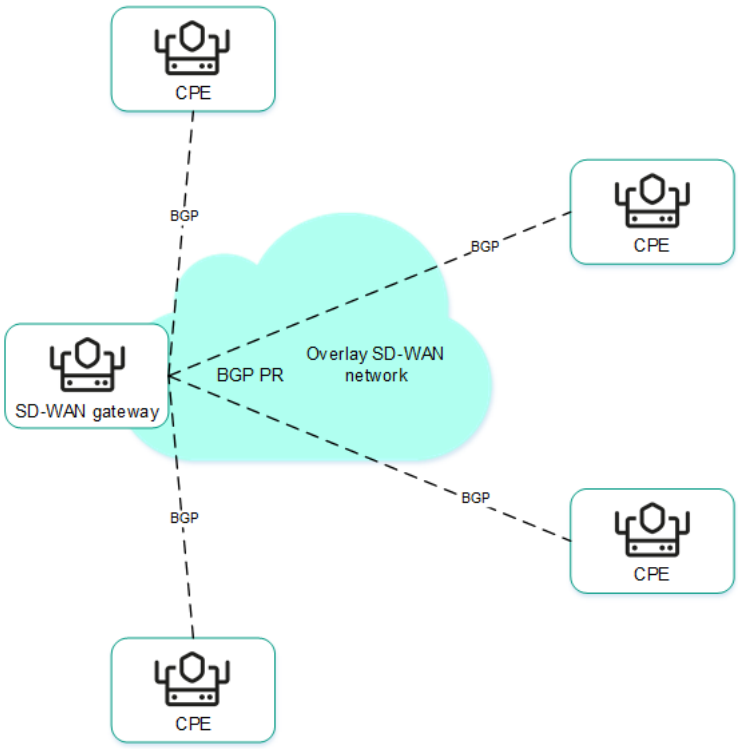
- Подключение нескольких клиентских площадок к сети L3 SD-WAN по BGP.



- Подключение устройств CPE к операторской сети IP/MPLS по BGP.



- Использование BGP для настройки связности устройств CPE внутри домена Kaspersky SD-WAN



Настройка протокола BGP

Вы можете указать параметры использования протокола динамической маршрутизации BGP на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Если вы планируете использовать фильтрацию маршрутов, перед настройкой протокола BGP требуется создать карты маршрутизации.

Для настройки протокола BGP используйте следующие инструкции:

- **Настройка протокола BGP на отдельном устройстве CPE**.

Чтобы настроить протокол BGP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры BGP**.

   По умолчанию выбрана вкладка **Общие параметры**, на которой отображаются параметры BGP.

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 **BGP** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

6. В поле **AS** введите номер вашей автономной системы. Диапазон значений: от 1 до 4 294 967 295.

7. В поле **CPE ID** введите IPv4-адрес устройства CPE.

8. В поле **Лимит маршрутов** введите максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 8.

9. При необходимости установите следующие флажки:

   - 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 одинаково на всех устройствах 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.

   - Установите флажок **IPv4 unicast-маршруты по умолчанию**, чтобы устройство CPE по умолчанию обменивалось IPv4-маршрутами с BGP-соседями.

   По умолчанию все флажки сняты.

10. При необходимости настройте BGP-таймеры:

    a. Установите флажок **BGP-таймеры**. По умолчанию флажок снят.

    b. В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений BGP-соседям. Диапазон значений: от 0 до 65 535.

c. В поле **Holdtime** введите время в секундах, в течение которого устройство CPE должно ожидать получения keepalive-сообщений от BGP-соседей. Если в течение указанного времени от BGP-соседа не поступает keepalive-сообщений, устройство считает его недоступным. Диапазон значений: от 0 до 65 535.

11. При необходимости в блоке **Перераспределение маршрутов** настройте перераспределение маршрутов других протоколов маршрутизации в BGP:

    a. Установите флажок рядом с типом маршрутов:

    - **Kernel** – перераспределять Kernel-маршруты, генерируемые операционной системой устройства CPE.
    - **Connected** – перераспределять маршруты, напрямую подключенные к интерфейсам устройства CPE.
    - **Статический** – перераспределять статические маршруты.
    - **OSPF** – перераспределять OSPF-маршруты.

    По умолчанию все флажки сняты.

    b. В раскрывающемся списке **Карта маршрутизации** выберите карту маршрутизации для определения маршрутов, которые требуется перераспределить.

    c. В поле **Метрика** введите метрику для перераспределяемых маршрутов. Диапазон значений: от 0 до 16 777 214.

12. При необходимости укажите сеть, которую устройство CPE должно анонсировать BGP-соседям:

    a. В блоке **Сети** нажмите на кнопку **+ Сеть**.

    b. В поле **Сеть** введите IP-адрес и маску подсети.

    c. В раскрывающемся списке **Карта маршрутизации** выберите карту маршрутизации для анонсируемых маршрутов.

    Вы можете указать несколько сетей.

13. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Настройка протокола BGP на всех устройствах, использующих шаблон CPE.

Чтобы настроить протокол BGP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры BGP**.

   По умолчанию выбрана вкладка **Общие параметры**, на которой отображаются параметры BGP.

4. В раскрывающемся списке **BGP** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

5. В поле **AS** введите номер вашей автономной системы. Диапазон значений: от 1 до 4 294 967 295.

6. В поле **CPE ID** введите IPv4-адрес устройства CPE.

7. В поле **Лимит маршрутов** введите максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 8.

8. 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 одинаково на всех устройствах 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.

   - Установите флажок **IPv4 unicast-маршруты по умолчанию**, чтобы устройство CPE по умолчанию обменивалось IPv4-маршрутами с BGP-соседями.

   По умолчанию все флажки сняты.

9. При необходимости настройте BGP-таймеры:

   a. Установите флажок **BGP-таймеры**. По умолчанию флажок снят.

   b. В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений BGP-соседям. Диапазон значений: от 0 до 65 535.

   c. В поле **Holdtime** введите время в секундах, в течение которого устройство CPE должно ожидать получения keepalive-сообщений от BGP-соседей. Если в течение указанного времени от BGP-соседа не поступает keepalive-сообщений, устройство считает его недоступным. Диапазон значений: от 0 до 65 535.

10. При необходимости в блоке **Перераспределение маршрутов** настройте перераспределение маршрутов других протоколов маршрутизации в BGP:

    a. Установите флажок рядом с типом маршрутов:

    - **Kernel** – перераспределять Kernel-маршруты, генерируемые операционной системой устройства CPE.
    - **Connected** – перераспределять маршруты, напрямую подключенные к интерфейсам устройства CPE.
    - **Статический** – перераспределять статические маршруты.
    - **OSPF** – перераспределять OSPF-маршруты.

    По умолчанию все флажки сняты.

    b. В раскрывающемся списке **Карта маршрутизации** выберите карту маршрутизации для определения маршрутов, которые требуется перераспределить.

    c. В поле **Метрика** введите метрику для перераспределяемых маршрутов. Диапазон значений: от 0 до 16 777 214.

11. При необходимости укажите сеть, которую устройство CPE должно анонсировать BGP-соседям:

    a. В блоке **Сети** нажмите на кнопку **+ Сеть**.

    b. В поле **Сеть** введите IP-адрес и маску подсети.

    c. В раскрывающемся списке **Карта маршрутизации** выберите карту маршрутизации для анонсируемых маршрутов.

    Вы можете указать несколько сетей.

12. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание BGP-соседа (BGP peer)

Вы можете создать BGP-соседа на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Максимальное количество динамических BGP-соседей: 512. Если вы планируете использовать фильтрацию маршрутов, перед созданием BGP-соседа требуется выполнить следующие действия:

- Создать списки управления доступом.
- Создать списки префиксов.
- Создать карты маршрутизации.

Для создания BGP-соседа используйте следующие инструкции:

- **Создание BGP-соседа на отдельном устройстве CPE**.

Чтобы создать BGP-соседа на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP** → **BGP-соседи**.

   Отобразится таблица BGP-соседей.

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 **+ BGP-сосед**.

6. В открывшемся окне в поле **Имя** введите имя BGP-соседа. Максимальная длина: 50 символов.

7. При необходимости не устанавливать TCP-сессию с BGP-соседом после создания установите флажок **Выключить BGP-соседа**. По умолчанию флажок снят.

8. В поле **IP соседа** введите IPv4-адрес BGP-соседа.

9. В поле **Удаленная AS** введите номер автономной системы BGP-соседа. Диапазон значений: от 1 до 4 294 967 295.

10. При необходимости в поле **Описание** введите краткое описание BGP-соседа.

11. В поле **Пароль** введите пароль для установления TCP-сессии с BGP-соседом. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра 👁. Для успешного установления TCP-сессии между двумя BGP-соседями они должны использовать одинаковый пароль.

12. В поле **Loopback-интерфейс** введите IP-адрес loopback-интерфейса, который устройство CPE должно передавать BGP-соседу при установлении TCP-сессии.

13. В поле **Хопы для eBGP** введите количество хопов (англ. hops) между устройством CPE и BGP-соседом, если TCP-сессия устанавливается не напрямую. Диапазон значений: от 1 до 255.

14. При необходимости настройте BGP-таймеры:

    a. Установите флажок **Уникальные BGP-таймеры**. По умолчанию флажок снят.

    b. В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений BGP-соседям. Диапазон значений: от 0 до 65 535.

    c. В поле **Holdtime** введите время в секундах, в течение которого устройство CPE должно ожидать получения keepalive-сообщений от BGP-соседей. Если в течение указанного времени от BGP-соседа не поступает keepalive-сообщений, устройство считает его недоступным. Диапазон значений: от 0 до 65 535.

15. При необходимости использовать протокол BFD для обнаружения потери связности установите флажок **BFD**. По умолчанию флажок снят.

16. Выберите вкладку **Расширенные параметры**, чтобы указать дополнительные параметры BGP-соседа.

17. При необходимости установите следующие флажки:

    - Установите флажок **Soft-reconfiguration inbound**, чтобы хранить анонсированные BGP-соседом маршруты локально на устройстве CPE. По умолчанию флажок снят.

      Использование этой функции снижает количество доступной на устройстве памяти.

    - 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 устройство CPE получало от BGP-соседа маршруты с атрибутом AS path, значением которого является номер автономной системы этого 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 IP-адрес устройства CPE в качестве 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 при настройке BGP-соседа, который находится в той же автономной системе, что устройство CPE.

    По умолчанию все флажки сняты.

18. 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.

19. В поле **Вес** введите вес маршрутов, анонсируемых BGP-соседом. Чем больше вес маршрута, тем больше его приоритет. Диапазон значений: от 0 до 65 535.

20. В поле **Лимит префиксов** введите максимальное количество префиксов, которое BGP-сосед может анонсировать устройству CPE. Диапазон значений: от 1 до 4 294 967 295.

21. Если требуется, чтобы устройство CPE анонсировало BGP-соседу маршруты с атрибутом community, установите флажок **Отправлять community** и в раскрывающемся списке выберите тип отправляемого атрибута:

    - **Все** – отправлять BGP-соседу все доступные типы атрибута community.

    - **Standard и extended community** – отправлять BGP-соседу атрибуты standard community и extended community.

    - **Extended community** – отправлять BGP-соседу атрибут extended community.

    - **Large community** – отправлять BGP-соседу атрибут large community.

- **Standard community** – отправлять BGP-соседу атрибут standard community.

По умолчанию флажок снят.

22. Установите флажок **Маршрут по умолчанию**, чтобы устройство CPE отправляло BGP-соседу маршрут по умолчанию: 0.0.0.0. По умолчанию флажок снят. Вы также можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать ранее созданную карту маршрутизации для маршрута по умолчанию.

23. Выберите вкладку **Фильтрация**, чтобы настроить фильтрацию маршрутов для BGP-соседа.

24. В блоке **Карта маршрутизации** выберите ранее созданные карты маршрутизации для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите карту маршрутизации, которую BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите карту маршрутизации, которую устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

25. В блоке **Список префиксов** выберите ранее созданные списки префиксов для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите список префиксов, который BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите список префиксов, который устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

26. В блоке **Список управления доступом** выберите ранее созданные списки управления доступом для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите список управления доступом, который BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите список управления доступом, который устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

27. Нажмите на кнопку **Создать**.

    BGP-сосед будет создан и отобразится в таблице.

28. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание BGP-соседа на всех устройствах, использующих шаблон CPE.

Чтобы создать BGP-соседа на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP → BGP-соседи**.

   Отобразится таблица BGP-соседей.

4. Нажмите на кнопку **+ BGP-сосед**.

5. В открывшемся окне в поле **Имя** введите имя BGP-соседа. Максимальная длина: 50 символов.

6. При необходимости не устанавливать TCP-сессию с BGP-соседом после создания установите флажок **Выключить BGP-соседа**. По умолчанию флажок снят.

7. В поле **IP соседа** введите IPv4-адрес BGP-соседа.

8. В поле **Удаленная AS** введите номер автономной системы BGP-соседа. Диапазон значений: от 1 до 4 294 967 295.

9. При необходимости в поле **Описание** введите краткое описание BGP-соседа.

10. В поле **Пароль** введите пароль для установления TCP-сессии с BGP-соседом. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра 👁. Для успешного установления TCP-сессии между двумя BGP-соседями они должны использовать одинаковый пароль.

11. В поле **Loopback-интерфейс** введите IP-адрес loopback-интерфейса, который устройство CPE должно передавать BGP-соседу при установлении TCP-сессии.

12. В поле **Хопы для eBGP** введите количество хопов (англ. hops) между устройством CPE и BGP-соседом, если TCP-сессия устанавливается не напрямую. Диапазон значений: от 1 до 255.

13. При необходимости настройте BGP-таймеры:

    a. Установите флажок **Уникальные BGP-таймеры**. По умолчанию флажок снят.

    b. В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений BGP-соседям. Диапазон значений: от 0 до 65 535.

    c. В поле **Holdtime** введите время в секундах, в течение которого устройство CPE должно ожидать получения keepalive-сообщений от BGP-соседей. Если в течение указанного времени от BGP-соседа не поступает keepalive-сообщений, устройство считает его недоступным. Диапазон значений: от 0 до 65 535.

14. При необходимости использовать протокол BFD для обнаружения потери связности установите флажок **BFD**. По умолчанию флажок снят.

15. Выберите вкладку **Расширенные параметры**, чтобы указать дополнительные параметры BGP-соседа.

16. При необходимости установите следующие флажки:

- Установите флажок **Soft-reconfiguration inbound**, чтобы хранить анонсированные BGP-соседом маршруты локально на устройстве CPE. По умолчанию флажок снят.

  Использование этой функции снижает количество доступной на устройстве памяти.

- 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 устройство CPE получало от BGP-соседа маршруты с атрибутом AS path, значением которого является номер автономной системы этого 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 IP-адрес устройства CPE в качестве 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 при настройке BGP-соседа, который находится в той же автономной системе, что устройство CPE.

По умолчанию все флажки сняты.

17. 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.

18. В поле **Вес** введите вес маршрутов, анонсируемых BGP-соседом. Чем больше вес маршрута, тем больше его приоритет. Диапазон значений: от 0 до 65 535.

19. В поле **Лимит префиксов** введите максимальное количество префиксов, которое BGP-сосед может анонсировать устройству CPE. Диапазон значений: от 1 до 4 294 967 295.

20. Если требуется, чтобы устройство CPE анонсировало BGP-соседу маршруты с атрибутом community, установите флажок **Отправлять community** и в раскрывающемся списке выберите тип отправляемого атрибута:

    - **Все** – отправлять BGP-соседу все доступные типы атрибута community.

    - **Standard и extended community** – отправлять BGP-соседу атрибуты standard community и extended community.

    - **Extended community** – отправлять BGP-соседу атрибут extended community.

    - **Large community** – отправлять BGP-соседу атрибут large community.

    - **Standard community** – отправлять BGP-соседу атрибут standard community.

    По умолчанию флажок снят.

21. Установите флажок **Маршрут по умолчанию**, чтобы устройство CPE отправляло BGP-соседу маршрут по умолчанию: 0.0.0.0. По умолчанию флажок снят. Вы также можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать ранее созданную карту маршрутизации для маршрута по умолчанию.

22. Выберите вкладку **Фильтрация**, чтобы настроить фильтрацию маршрутов для BGP-соседа.

23. В блоке **Карта маршрутизации** выберите ранее созданные карты маршрутизации для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите карту маршрутизации, которую BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите карту маршрутизации, которую устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

24. В блоке **Список префиксов** выберите ранее созданные списки префиксов для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите список префиксов, который BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите список префиксов, который устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

25. В блоке **Список управления доступом** выберите ранее созданные списки управления доступом для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите список управления доступом, который BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите список управления доступом, который устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

26. Нажмите на кнопку **Создать**.

    BGP-сосед будет создан и отобразится в таблице.

27. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение BGP-соседа

Вы можете изменить BGP-соседа на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию BGP-соседа.

Чтобы изменить BGP-соседа на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP → BGP-соседи**.

   Отобразится таблица BGP-соседей.

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 **Изменить** рядом с BGP-соседом.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить BGP-соседа на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP → BGP-соседи**.

   Отобразится таблица BGP-соседей.

4. Нажмите на кнопку **Изменить** рядом с BGP-соседом.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление BGP-соседа

Вы можете удалить BGP-соседа на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленных BGP-соседей невозможно восстановить.

Чтобы удалить BGP-соседа на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP → BGP-соседи**.

   Отобразится таблица BGP-соседей.

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 **Удалить** рядом с BGP-соседом.

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

   BGP-сосед будет удален и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить BGP-соседа на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP → BGP-соседи**.

   Отобразится таблица BGP-соседей.

4. Нажмите на кнопку **Удалить** рядом с BGP-соседом.

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

   BGP-сосед будет удален и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание группы BGP-соседей (BGP peer group)

Вы можете создать группу BGP-соседей на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Если вы планируете использовать фильтрацию маршрутов, перед созданием группы BGP-соседей требуется выполнить следующие действия:

- Создать списки управления доступом.
- Создать списки префиксов.
- Создать карты маршрутизации.

Для создания группы BGP-соседей используйте следующие инструкции:

- **Создание группы BGP-соседей на отдельном устройстве CPE**.

Чтобы создать группу BGP-соседей на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP** → **Группы BGP-соседей**.

   Отобразится таблица групп BGP-соседей.

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 **+ Группа BGP-соседей**.

6. В открывшемся окне в поле **Имя** введите имя группы BGP-соседей. Максимальная длина: 50 символов.

7. При необходимости не устанавливать TCP-сессию с группой BGP-соседей после ее создания установите флажок **Выключить группу BGP-соседей**. По умолчанию флажок снят.

8. В поле **Диапазон BGP** введите диапазон IP-адресов группы BGP-соседей. Диапазон определяется с помощью префикса.

9. В поле **Удаленная AS** введите номер автономной системы группы BGP-соседей. Диапазон значений: от 1 до 4 294 967 295.

10. При необходимости в поле **Описание** введите краткое описание группы BGP-соседей.

11. В поле **Пароль** введите пароль для установления TCP-сессии с группой BGP-соседей. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра 👁. Для успешного установления TCP-сессии между двумя BGP-соседями они должны использовать одинаковый пароль.

12. В поле **Loopback-интерфейс** введите IP-адрес loopback-интерфейса, который устройство CPE должно передавать группе BGP-соседей при установлении TCP-сессии.

13. В поле **Хопы для eBGP** введите количество хопов (англ. hops) между устройством CPE и группой BGP-соседей, если TCP-сессия устанавливается не напрямую. Диапазон значений: от 1 до 255.

14. При необходимости настройте BGP-таймеры:

    a. Установите флажок **Уникальные BGP-таймеры**. По умолчанию флажок снят.

    b. В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений группе BGP-соседей. Диапазон значений: от 0 до 65 535.

    c. В поле **Holdtime** введите время в секундах, в течение которого устройство CPE должно ожидать получения keepalive-сообщений от группы BGP-соседей. Если в течение указанного времени от BGP-соседа не поступает keepalive-сообщений, устройство считает его недоступным. Диапазон значений: от 0 до 65 535.

15. При необходимости использовать протокол BFD для обнаружения потери связности установите флажок **BFD**. По умолчанию флажок снят.

16. Выберите вкладку **Расширенные параметры**, чтобы указать дополнительные параметры группы BGP-соседей.

17. 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 доступной на устройстве памяти.

    - 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 устройство CPE получало от группы BGP-соседей маршруты с атрибутом AS path, значением которого является номер автономной системы этого 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 IP-адрес устройства CPE в качестве 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 при настройке группы BGP-соседей, которая находится в той же автономной системе, что устройство CPE.

    По умолчанию все флажки сняты.

18. 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.

19. 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.

20. В поле **Лимит префиксов** введите максимальное количество префиксов, которое группа BGP-соседей может анонсировать устройству CPE. Диапазон значений: от 1 до 4 294 967 295.

21. Если требуется, чтобы устройство CPE анонсировало группе BGP-соседей маршруты с атрибутом community, установите флажок **Отправлять community** и в раскрывающемся списке выберите тип отправляемого атрибута:

    - **Все** – отправлять BGP-соседу все доступные типы атрибута community.

    - **Standard и extended community** – отправлять BGP-соседу атрибуты standard community и extended community.

    - **Extended community** – отправлять BGP-соседу атрибут extended community.

- **Large community** – отправлять BGP-соседу атрибут large community.
- **Standard community** – отправлять BGP-соседу атрибут standard community.

По умолчанию флажок снят.

22. Установите флажок **Маршрут по умолчанию**, чтобы устройство CPE отправляло группе BGP-соседей маршрут по умолчанию: 0.0.0.0. По умолчанию флажок снят. Вы также можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать ранее созданную карту маршрутизации для маршрута по умолчанию.
23. Выберите вкладку **Фильтрация**, чтобы настроить фильтрацию маршрутов для группы BGP-соседей.
24. В блоке **Карта маршрутизации** выберите ранее созданные карты маршрутизации для фильтрации маршрутов:
    a. В раскрывающемся списке **Входящие** выберите карту маршрутизации, которую группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.
    b. В раскрывающемся списке **Исходящие** выберите карту маршрутизации, которую устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.
25. В блоке **Список префиксов** выберите ранее созданные списки префиксов для фильтрации маршрутов:
    a. В раскрывающемся списке **Входящие** выберите список префиксов, который группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.
    b. В раскрывающемся списке **Исходящие** выберите список префиксов, который устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.
26. В блоке **Список управления доступом** выберите ранее созданные списки управления доступом для фильтрации маршрутов:
    a. В раскрывающемся списке **Входящие** выберите список управления доступом, который группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.
    b. В раскрывающемся списке **Исходящие** выберите список управления доступом, который устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.
27. Нажмите на кнопку **Создать**.

    Группа BGP-соседей будет создана и отобразится в таблице.
28. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание группы BGP-соседей на всех устройствах, использующих шаблон CPE.

Чтобы создать группу BGP-соседей на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP → Группы BGP-соседей**.

   Отобразится таблица групп BGP-соседей.

4. Нажмите на кнопку **+ Группа BGP-соседей**.

5. В открывшемся окне в поле **Имя** введите имя группы BGP-соседей. Максимальная длина: 50 символов.

6. При необходимости не устанавливать TCP-сессию с группой BGP-соседей после ее создания установите флажок **Выключить группу BGP-соседей**. По умолчанию флажок снят.

7. В поле **Диапазон BGP** введите диапазон IP-адресов группы BGP-соседей. Диапазон определяется с помощью префикса.

8. В поле **Удаленная AS** введите номер автономной системы группы BGP-соседей. Диапазон значений: от 1 до 4 294 967 295.

9. При необходимости в поле **Описание** введите краткое описание группы BGP-соседей.

10. В поле **Пароль** введите пароль для установления TCP-сессии с группой BGP-соседей. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра 👁. Для успешного установления TCP-сессии между двумя BGP-соседями они должны использовать одинаковый пароль.

11. В поле **Loopback-интерфейс** введите IP-адрес loopback-интерфейса, который устройство CPE должно передавать группе BGP-соседей при установлении TCP-сессии.

12. В поле **Хопы для eBGP** введите количество хопов (англ. hops) между устройством CPE и группой BGP-соседей, если TCP-сессия устанавливается не напрямую. Диапазон значений: от 1 до 255.

13. При необходимости настройте BGP-таймеры:

    a. Установите флажок **Уникальные BGP-таймеры**. По умолчанию флажок снят.

    b. В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений группе BGP-соседей. Диапазон значений: от 0 до 65 535.

    c. В поле **Holdtime** введите время в секундах, в течение которого устройство CPE должно ожидать получения keepalive-сообщений от группы BGP-соседей. Если в течение указанного времени от BGP-соседа не поступает keepalive-сообщений, устройство считает его недоступным. Диапазон значений: от 0 до 65 535.

14. При необходимости использовать протокол BFD для обнаружения потери связности установите флажок **BFD**. По умолчанию флажок снят.

15. Выберите вкладку **Расширенные параметры**, чтобы указать дополнительные параметры группы BGP-соседей.

16. 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 доступной на устройстве памяти.

    - 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 устройство CPE получало от группы BGP-соседей маршруты с атрибутом AS path, значением которого является номер автономной системы этого 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 IP-адрес устройства CPE в качестве 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 при настройке группы BGP-соседей, которая находится в той же автономной системе, что устройство CPE.

    По умолчанию все флажки сняты.

17. 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.

18. 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.

19. В поле **Лимит префиксов** введите максимальное количество префиксов, которое группа BGP-соседей может анонсировать устройству CPE. Диапазон значений: от 1 до 4 294 967 295.

20. Если требуется, чтобы устройство CPE анонсировало группе BGP-соседей маршруты с атрибутом community, установите флажок **Отправлять community** и в раскрывающемся списке выберите тип отправляемого атрибута:

    - **Все** – отправлять BGP-соседу все доступные типы атрибута community.

    - **Standard и extended community** – отправлять BGP-соседу атрибуты standard community и extended community.

    - **Extended community** – отправлять BGP-соседу атрибут extended community.

    - **Large community** – отправлять BGP-соседу атрибут large community.

    - **Standard community** – отправлять BGP-соседу атрибут standard community.

    По умолчанию флажок снят.

21. Установите флажок **Маршрут по умолчанию**, чтобы устройство CPE отправляло группе BGP-соседей маршрут по умолчанию: 0.0.0.0. По умолчанию флажок снят. Вы также можете установить флажок **Применять карту маршрутизации** и в отобразившемся раскрывающемся списке выбрать ранее созданную карту маршрутизации для маршрута по умолчанию.

22. Выберите вкладку **Фильтрация**, чтобы настроить фильтрацию маршрутов для группы BGP-соседей.

23. В блоке **Карта маршрутизации** выберите ранее созданные карты маршрутизации для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите карту маршрутизации, которую группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите карту маршрутизации, которую устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.

24. В блоке **Список префиксов** выберите ранее созданные списки префиксов для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите список префиксов, который группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите список префиксов, который устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.

25. В блоке **Список управления доступом** выберите ранее созданные списки управления доступом для фильтрации маршрутов:

    a. В раскрывающемся списке **Входящие** выберите список управления доступом, который группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.

    b. В раскрывающемся списке **Исходящие** выберите список управления доступом, который устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.

26. Нажмите на кнопку **Создать**.

    Группа BGP-соседей будет создана и отобразится в таблице.

27. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение группы BGP-соседей

Вы можете изменить группу BGP-соседей на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию группы BGP-соседей.

Чтобы изменить группу BGP-соседей на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP** → **Группы BGP-соседей**.

   Отобразится таблица групп BGP-соседей.

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 **Изменить** рядом с группой BGP-соседей.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить группу BGP-соседей на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP** → **Группы BGP-соседей**.

   Отобразится таблица групп BGP-соседей.

4. Нажмите на кнопку **Изменить** рядом с группой BGP-соседей.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление группы BGP-соседей

Вы можете удалить группу BGP-соседей на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные группы BGP-соседей невозможно восстановить.

Чтобы удалить группу BGP-соседей на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP** → **Группы BGP-соседей**.

   Отобразится таблица групп BGP-соседей.

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 **Удалить** рядом с группой BGP-соседей.

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

   Группа BGP-соседей будет удалена и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить группу BGP-соседей на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BGP** → **Группы BGP-соседей**.

   Отобразится таблица групп BGP-соседей.

4. Нажмите на кнопку **Удалить** рядом с группой BGP-соседей.

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

   Группа BGP-соседей будет удалена и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Протокол динамической маршрутизации OSPF

Kaspersky SD-WAN поддерживает использование протокола динамической маршрутизации OSPF (Open Shortest Path First) для обмена маршрутной информацией между подключенными к вашей сети SD-WAN устройствами CPE, а также со сторонними сетевыми устройствами.

При настройке протокола можете создать OSPF-области (англ. OSPF areas, далее также области) и OSPF-интерфейсы (далее также интерфейсы).

Настройка протокола OSPF

Вы можете указать параметры использования протокола динамической маршрутизации OSPF на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Если вы планируете использовать фильтрацию маршрутов, перед настройкой протокола OSPF требуется выполнить следующие действия:

- Создать карты маршрутизации.

- Создать списки управления доступом.
- Создать списки префиксов.

Для настройки протокола OSPF используйте следующие инструкции:

- **Настройка протокола OSPF на отдельном устройстве CPE**.

Чтобы настроить протокол OSPF на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF**.

   По умолчанию выбрана вкладка **Общие параметры**, на которой отображаются параметры OSPF.

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 **OSPF** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

6. В поле **CPE ID** введите IPv4-адрес устройства CPE.

7. В поле **Максимум путей** введите максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 16.

8. При необходимости использовать устройство CPE как пограничный маршрутизатор (англ. Area Border Router, ABR) в раскрывающемся списке **Тип ABR** выберите одно из следующих значений:

   - **IBM** – эта имплементация используется по умолчанию.
   - **CISCO**.
   - **Использовать сокращенные маршруты**.
   - **STANDARD**.

9. В поле **Пропускная способность для автоопределения стоимости** введите контрольное значение пропускной способности для подсчета стоимости каналов связи. С помощью стоимости определяется наилучший маршрут. Вы можете снижать или повышать контрольное значение, чтобы влиять на выбор маршрутов и отдавать предпочтение определенным каналам связи. Диапазон значений: от 1 до 4 294 967.

10. При необходимости перевести все интерфейсы устройства CPE в пассивный режим установите флажок **Пассивные интерфейсы по умолчанию**. В пассивном режиме интерфейсы не отправляют OSPF hello-пакеты и активно не участвуют в OSPF-маршрутизации. Как правило, в пассивный режим переводятся интерфейсы, которые не нуждаются в обновлениях маршрутной информации, например интерфейсы, подключенные к пользовательским устройствам или сетям, не входящим в OSPF-домен. По умолчанию флажок снят.

11. При необходимости вести журнал OSPF установите флажок **Вести журнал изменений смежности**. В журнал OSPF вносятся изменения, происходящие между устройством CPE и OSPF-соседями, например когда сосед выходит из строя. Этот флажок позволяет отслеживать

изменения, решать проблемы, связанные с работой соседей, а также собирать информацию о стабильности OSPF-сети. По умолчанию флажок снят.

12. Если вы установили флажок **Вести журнал изменений смежности**, при необходимости вести более подробный журнал OSPF установите флажок **Подробный журнал**. Более подробный журнал позволяет произвести диагностику отдельных событий, происходящих с OSPF-соседом, а также просмотреть, в какой последовательности изменяются его состояния. По умолчанию флажок снят.

13. При необходимости в блоке **Перераспределение маршрутов** настройте перераспределение маршрутов других протоколов маршрутизации в OSPF:

    a. Установите флажок рядом с типом маршрутов:

    - **BGP** – перераспределять BGP-маршруты.
    - **Connected** – перераспределять маршруты, напрямую подключенные к интерфейсам устройства CPE.
    - **Kernel** – перераспределять Kernel-маршруты, генерируемые операционной системой устройства CPE.
    - **Статический** – перераспределять статические маршруты.

    По умолчанию все флажки сняты.

    b. В раскрывающемся списке **Карта маршрутизации** выберите ранее созданную карту маршрутизации для определения маршрутов, которые требуется перераспределить.

    c. В поле **Метрика** введите метрику для 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, в соответствии с которым требуется перераспределять маршруты. По умолчанию флажок снят.

14. В поле **Метрика по умолчанию** введите метрику по умолчанию для всех OSPF-маршрутов. Диапазон значений: от 0 до 16 777 214.

15. При необходимости настройте анонсирование устройством CPE маршрута по умолчанию в OSPF-сеть:

    a. Установите флажок **Объявлять маршрут по умолчанию**. По умолчанию флажок снят.

    b. Установите флажок **Применять всегда**, чтобы всегда анонсировать маршрут по умолчанию, 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:

    - **Type 1**.

- **Type 2**.

d. В поле **Метрика** введите метрику для маршрута по умолчанию. Диапазон значений: от 0 до 16 777 214.

e. В раскрывающемся списке **Карта маршрутизации** выберите ранее созданную карту маршрутизации для маршрута по умолчанию.

16. В поле **Дистанция** введите административную дистанцию для OSPF-маршрутов. Когда до одного назначения существует несколько маршрутов, полученных из разных протоколов маршрутизации, *административная дистанция* позволяет определить протокол, которому требуется отдать предпочтение.

    Чем ниже значение административной дистанции, указанное для протокола, тем выше приоритет его маршрутов. Например, если вы хотите, чтобы маршрутам, полученным из OSPF, всегда отдавалось предпочтение по отношению к маршрутам, полученным из BGP, укажите административную дистанцию 1 для OSPF и 2 для BGP. Диапазон значений: от 1 до 255.

17. При необходимости настройте административные дистанции отдельных OSPF-маршрутов:

    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.

18. При необходимости включите перезагрузку Graceful restart на устройстве CPE:

    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 анонсирует намерение выполнить перезагрузку OSPF-соседям. Диапазон значений: от 1 до 1800.

19. При необходимости настройте таймеры для вычислений алгоритма Shortest Path First (SPF, далее SPF-алгоритм):

    a. Установите флажок **Таймер ограничения частоты SPF**. По умолчанию флажок снят.

    b. В поле **Задержка (мсек.)** 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.

20. При необходимости настройте максимальные метрики для объявлений о состоянии канала (англ. Link State Advertisement, далее LSA):

a. Установите флажок **По требованию администратора**, чтобы административно указать максимальное значение метрики для LSA устройства CPE.

b. Установите флажок **При запуске**, чтобы указать время в секундах, в течение которого максимальная метрика остается примененной к LSA устройства CPE при запуске или перезапуске OSPF-процесса, и в поле **Таймер (сек.)** введите требуемое значение.

c. Установите флажок **При выключении**, чтобы указать время в секундах, в течение которого максимальная метрика остается примененной к LSA устройства CPE при завершении OSPF-процесса, и в поле **Таймер (сек.)** введите требуемое значение.

21. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Настройка протокола OSPF на всех устройствах, использующих шаблон CPE.

Чтобы настроить протокол OSPF на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF**.

   По умолчанию выбрана вкладка **Общие параметры**, на которой отображаются параметры OSPF.

4. В раскрывающемся списке **OSPF** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

5. В поле **CPE ID** введите IPv4-адрес устройства CPE.

6. В поле **Максимум путей** введите максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 16.

7. При необходимости использовать устройство CPE как пограничный маршрутизатор (англ. Area Border Router, ABR) в раскрывающемся списке **Тип ABR** выберите одно из следующих значений:

   - **IBM** – эта имплементация используется по умолчанию.
   - **CISCO**.
   - **Использовать сокращенные маршруты**.
   - **STANDARD**.

8. В поле **Пропускная способность для автоопределения стоимости** введите контрольное значение пропускной способности для подсчета стоимости каналов связи. С помощью стоимости определяется наилучший маршрут. Вы можете снижать или повышать контрольное значение, чтобы влиять на выбор маршрутов и отдавать предпочтение определенным каналам связи. Диапазон значений: от 1 до 4 294 967.

9. При необходимости перевести все интерфейсы устройства CPE в пассивный режим установите флажок **Пассивные интерфейсы по умолчанию**. В пассивном режиме интерфейсы не отправляют OSPF hello-пакеты и активно не участвуют в OSPF-маршрутизации. Как правило, в пассивный режим переводятся интерфейсы, которые не нуждаются в обновлениях маршрутной информации, например интерфейсы, подключенные к пользовательским устройствам или сетям, не входящим в OSPF-домен. По умолчанию флажок снят.

10. При необходимости вести журнал OSPF установите флажок **Вести журнал изменений смежности**. В журнал OSPF вносятся изменения, происходящие между устройством CPE и OSPF-соседями, например когда сосед выходит из строя. Этот флажок позволяет отслеживать изменения, решать проблемы, связанные с работой соседей, а также собирать информацию о стабильности OSPF-сети. По умолчанию флажок снят.

11. Если вы установили флажок **Вести журнал изменений смежности**, при необходимости вести более подробный журнал OSPF установите флажок **Подробный журнал**. Более подробный

журнал позволяет произвести диагностику отдельных событий, происходящих с OSPF-соседом, а также просмотреть, в какой последовательности изменяются его состояния. По умолчанию флажок снят.

12. При необходимости в блоке **Перераспределение маршрутов** настройте перераспределение маршрутов других протоколов маршрутизации в OSPF:

    a. Установите флажок рядом с типом маршрутов:

    - **BGP** – перераспределять BGP-маршруты.
    - **Connected** – перераспределять маршруты, напрямую подключенные к интерфейсам устройства CPE.
    - **Kernel** – перераспределять Kernel-маршруты, генерируемые операционной системой устройства CPE.
    - **Статический** – перераспределять статические маршруты.

    По умолчанию все флажки сняты.

    b. В раскрывающемся списке **Карта маршрутизации** выберите ранее созданную карту маршрутизации для определения маршрутов, которые требуется перераспределить.

    c. В поле **Метрика** введите метрику для 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, в соответствии с которым требуется перераспределять маршруты. По умолчанию флажок снят.

13. В поле **Метрика по умолчанию** введите метрику по умолчанию для всех OSPF-маршрутов. Диапазон значений: от 0 до 16 777 214.

14. При необходимости настройте анонсирование устройством CPE маршрута по умолчанию в OSPF-сеть:

    a. Установите флажок **Объявлять маршрут по умолчанию**. По умолчанию флажок снят.

    b. Установите флажок **Применять всегда**, чтобы всегда анонсировать маршрут по умолчанию, 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:

    - **Type 1**.
    - **Type 2**.

    d. В поле **Метрика** введите метрику для маршрута по умолчанию. Диапазон значений: от 0 до 16 777 214.

e. В раскрывающемся списке **Карта маршрутизации** выберите ранее созданную карту маршрутизации для маршрута по умолчанию.

15. В поле **Дистанция** введите административную дистанцию для OSPF-маршрутов. Когда до одного назначения существует несколько маршрутов, полученных из разных протоколов маршрутизации, *административная дистанция* позволяет определить протокол, которому требуется отдать предпочтение.

    Чем ниже значение административной дистанции, указанное для протокола, тем выше приоритет его маршрутов. Например, если вы хотите, чтобы маршрутам, полученным из OSPF, всегда отдавалось предпочтение по отношению к маршрутам, полученным из BGP, укажите административную дистанцию 1 для OSPF и 2 для BGP. Диапазон значений: от 1 до 255.

16. При необходимости настройте административные дистанции отдельных OSPF-маршрутов:

    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.

17. При необходимости включите перезагрузку Graceful restart на устройстве CPE:

    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 анонсирует намерение выполнить перезагрузку OSPF-соседям. Диапазон значений: от 1 до 1800.

18. При необходимости настройте таймеры для вычислений алгоритма Shortest Path First (SPF, далее SPF-алгоритм):

    a. Установите флажок **Таймер ограничения частоты SPF**. По умолчанию флажок снят.

    b. В поле **Задержка (мсек.)** 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.

19. При необходимости настройте максимальные метрики для объявлений о состоянии канала (англ. Link State Advertisement, далее LSA):

    a. Установите флажок **По требованию администратора**, чтобы административно указать максимальное значение метрики для LSA устройства CPE.

    b. Установите флажок **При запуске**, чтобы указать время в секундах, в течение которого максимальная метрика остается примененной к LSA устройства CPE при запуске или

перезапуске OSPF-процесса, и в поле **Таймер (сек.)** введите требуемое значение.

c. Установите флажок **При выключении**, чтобы указать время в секундах, в течение которого максимальная метрика остается примененной к LSA устройства CPE при завершении OSPF-процесса, и в поле **Таймер (сек.)** введите требуемое значение.

20. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание OSPF-области

Вы можете создать OSPF-область на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Если вы планируете использовать фильтрацию маршрутов, перед созданием области требуется выполнить следующие действия:

- Создать списки управления доступом.
- Создать списки префиксов.

Для создания OSPF-области используйте следующие инструкции:

- **Создание OSPF-области на отдельном устройстве CPE**.

Чтобы создать OSPF-область на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF** → **OSPF-области**.

   Отобразится таблица OSPF-областей.

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 **+ Конфигурирование OSPF-области**.

6. В открывшемся окне в поле **Имя** введите идентификатор области в формате IPv4-адреса или целого числа.

7. При необходимости сделайте область тупиковой (англ. stub area):

   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 распространение маршрута по умолчанию в NSSA-область установите флажок **Подавлять FA в NSSA**. По умолчанию флажок снят.

   d. В поле **Стоимость по умолчанию** введите метрику для маршрута по умолчанию или для суммированных маршрутов.

8. При необходимости использовать метод кратчайшего маршрута (англ. shortcut), когда выполняются вычисления SPF-алгоритма, установите флажок **Использовать сокращенные маршруты**. Этот метод позволяет снизить количество выполняемых вычислений за счет исключения определенных областей. По умолчанию флажок снят.

9. В раскрывающемся списке **Аутентификация** выберите метод аутентификации в OSPF:

   - **Хеш-функция** – использовать MD5-алгоритм, который обеспечивает безопасность взаимодействия за счет подтверждения подлинности пакетов с помощью общего секретного ключа.
   - **Пароль** – использовать незашифрованный пароль. Этот метод аутентификации является менее надежным по сравнению с **Хеш-функция**, однако он может обеспечить аутентификацию при

использовании в доверенном сетевом окружении.

10. При необходимости в блоке **OSPF-диапазоны** добавьте диапазон IP-адресов и разрешите или запретите анонсирование адресов из этого диапазона в OSPF:

    a. Нажмите на кнопку **+ Диапазон**.

    b. В поле **Диапазон** введите диапазон IP-адресов. Диапазон определяется с помощью префикса.

    c. В раскрывающемся списке **Действие** выберите действие, которое требуется применять к IP-адресам из диапазона:

    - **Объявлять** – анонсировать в OSPF. Это значение выбрано по умолчанию.
    - **Не объявлять** – не анонсировать в OSPF.
    - **Заменять** – заменить на IP-адреса из другого диапазона и анонсировать в OSPF.

    d. Если в раскрывающемся списке **Действие** вы выбрали **Заменять**, в поле **Заменять** введите диапазон IP-адресов, которым требуется заменить оригинальный диапазон.

    e. Если в раскрывающемся списке **Действие** вы выбрали **Объявлять** или **Заменять**, в поле **Стоимость** введите метрику для IP-адресов из диапазона. Диапазон значений: от 0 до 16 777 215.

11. При необходимости в блоке **Виртуальные соединения** добавьте виртуальный канал связи, чтобы соединить создаваемую область с другой областью через транзитную область:

    a. Нажмите на кнопку **+ Виртуальное соединение**.

    b. В поле **Адрес** введите IPv4-адрес интерфейса маршрутизатора в транзитной области.

12. При необходимости в блоке **Фильтрация** настройте фильтрацию маршрутов в OSPF:

    a. В раскрывающемся списке **Список экспорта** выберите ранее созданный список управления доступом для фильтрации маршрутов, анонсируемых в другие области.

    b. В раскрывающемся списке **Список импорта** выберите ранее созданный список управления доступом для фильтрации маршрутов, анонсируемых из других областей.

    c. В раскрывающемся списке **Исходящий список фильтрации** выберите ранее созданный список префиксов для фильтрации маршрутов, анонсируемых в другие области.

    d. В раскрывающемся списке **Входящий список фильтрации** выберите ранее созданный список префиксов для фильтрации маршрутов, анонсируемых из других областей.

13. Нажмите на кнопку **Сохранить**.

    OSPF-область будет создана и отобразится в таблице.

14. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание OSPF-области на всех устройствах, использующих шаблон CPE.

Чтобы создать OSPF-область на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF → OSPF-области**.

   Отобразится таблица OSPF-областей.

4. Нажмите на кнопку **+ Конфигурирование OSPF-области**.

5. В открывшемся окне в поле **Имя** введите идентификатор области в формате IPv4-адреса или целого числа.

6. При необходимости сделайте область тупиковой (англ. stub area):

   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 распространение маршрута по умолчанию в NSSA-область установите флажок **Подавлять FA в NSSA**. По умолчанию флажок снят.

   d. В поле **Стоимость по умолчанию** введите метрику для маршрута по умолчанию или для суммированных маршрутов.

7. При необходимости использовать метод кратчайшего маршрута (англ. shortcut), когда выполняются вычисления SPF-алгоритма, установите флажок **Использовать сокращенные маршруты**. Этот метод позволяет снизить количество выполняемых вычислений за счет исключения определенных областей. По умолчанию флажок снят.

8. В раскрывающемся списке **Аутентификация** выберите метод аутентификации в OSPF:

   - **Хеш-функция** – использовать MD5-алгоритм, который обеспечивает безопасность взаимодействия за счет подтверждения подлинности пакетов с помощью общего секретного ключа.
   - **Пароль** – использовать незашифрованный пароль. Этот метод аутентификации является менее надежным по сравнению с **Хеш-функция**, однако он может обеспечить аутентификацию при использовании в доверенном сетевом окружении.

9. При необходимости в блоке **OSPF-диапазоны** добавьте диапазон IP-адресов и разрешите или запретите анонсирование адресов из этого диапазона в OSPF:

a. Нажмите на кнопку **+ Диапазон**.

b. В поле **Диапазон** введите диапазон IP-адресов. Диапазон определяется с помощью префикса.

c. В раскрывающемся списке **Действие** выберите действие, которое требуется применять к IP-адресам из диапазона:

- **Объявлять** – анонсировать в OSPF. Это значение выбрано по умолчанию.
- **Не объявлять** – не анонсировать в OSPF.
- **Заменять** – заменить на IP-адреса из другого диапазона и анонсировать в OSPF.

d. Если в раскрывающемся списке **Действие** вы выбрали **Заменять**, в поле **Заменять** введите диапазон IP-адресов, которым требуется заменить оригинальный диапазон.

e. Если в раскрывающемся списке **Действие** вы выбрали **Объявлять** или **Заменять**, в поле **Стоимость** введите метрику для IP-адресов из диапазона. Диапазон значений: от 0 до 16 777 215.

10. При необходимости в блоке **Виртуальные соединения** добавьте виртуальный канал связи, чтобы соединить создаваемую область с другой областью через транзитную область:

a. Нажмите на кнопку **+ Виртуальное соединение**.

b. В поле **Адрес** введите IPv4-адрес интерфейса маршрутизатора в транзитной области.

11. При необходимости в блоке **Фильтрация** настройте фильтрацию маршрутов в OSPF:

a. В раскрывающемся списке **Список экспорта** выберите ранее созданный список управления доступом для фильтрации маршрутов, анонсируемых в другие области.

b. В раскрывающемся списке **Список импорта** выберите ранее созданный список управления доступом для фильтрации маршрутов, анонсируемых из других областей.

c. В раскрывающемся списке **Исходящий список фильтрации** выберите ранее созданный список префиксов для фильтрации маршрутов, анонсируемых в другие области.

d. В раскрывающемся списке **Входящий список фильтрации** выберите ранее созданный список префиксов для фильтрации маршрутов, анонсируемых из других областей.

12. Нажмите на кнопку **Сохранить**.

OSPF-область будет создана и отобразится в таблице.

13. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение OSPF-области

Вы можете изменить OSPF-область на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию области.

Чтобы изменить OSPF-область на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF → OSPF-области**.

   Отобразится таблица OSPF-областей.

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 **Изменить** рядом с OSPF-областью.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить OSPF-область на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF → OSPF-области**.

   Отобразится таблица OSPF-областей.

4. Нажмите на кнопку **Изменить** рядом с OSPF-областью.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление OSPF-области

Вы можете удалить OSPF-область на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные области невозможно восстановить.

Чтобы удалить OSPF-область на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **OSPF** → **OSPF-области**.

   Отобразится таблица OSPF-областей.

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 **Удалить** рядом с OSPF-областью.

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

   OSPF-область будет удалена и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить OSPF-область на всех устройствах, использующих шаблон CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **OSPF** → **OSPF-области**.

   Отобразится таблица OSPF-областей.

4. Нажмите на кнопку **Удалить** рядом с OSPF-областью.

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

   OSPF-область будет удалена и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание OSPF-интерфейса

Вы можете создать OSPF-интерфейс на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. OSPF-интерфейсы создаются поверх сетевых интерфейсов, поэтому сначала требуется создать сетевой интерфейс.

Для создания OSPF-интерфейса используйте следующие инструкции:

- Создание OSPF-интерфейса на отдельном устройстве CPE.

Чтобы создать OSPF-интерфейс на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF** → **OSPF-интерфейсы**.

   Отобразится таблица OSPF-интерфейсов.

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 **+ Конфигурирование OSPF-интерфейса**.

6. В открывшемся окне в раскрывающемся списке **Интерфейс** выберите ранее созданный сетевой интерфейс, поверх которого требуется создать OSPF-интерфейс.

7. В поле **OSPF-область** введите идентификатор OSPF-области, к которой относится интерфейс, в формате IPv4-адреса или целого числа.

8. При необходимости настройте аутентификацию в OSPF:

   a. В раскрывающемся списке **Аутентификация** выберите метод аутентификации:

      - **Хеш-функция** – использовать MD5-алгоритм, который обеспечивает безопасность взаимодействия за счет подтверждения подлинности пакетов с помощью общего секретного ключа.

      - **Пароль** – использовать незашифрованный пароль. Этот метод аутентификации является менее надежным по сравнению с **Хеш-функция**, однако он может обеспечить аутентификацию при использовании в доверенном сетевом окружении.

   b. Если в раскрывающемся списке **Аутентификация** вы выбрали **Хеш-функция**, в поле **Пароль** введите пароль для аутентификации.

   c. Если в раскрывающемся списке **Аутентификация** вы выбрали **Хеш-функция**, выполните следующие действия:

      1. В поле **Key ID** введите MD5-хеш. Диапазон значений: от 1 до 255.

      2. В поле **Ключ** введите MD5-ключ.

9. В поле **Стоимость** введите метрику интерфейса. Диапазон значений: от 1 до 65 535.

10. В раскрывающемся списке **Тип сети** выберите тип сети, связанной с интерфейсом:

    - **Широковещательная**.

    - **Не широковещательная**.

    - **point-to-multipoint**.

- **point-to-point**.

11. В поле **Приоритет** введите приоритет интерфейса. Устройство CPE с наивысшим приоритетом интерфейса становится выделенным маршрутизатором (англ. designated router), в то время как устройство со вторым по величине приоритетом становится резервным выделенным маршрутизатором (англ. backup designated router).

12. При необходимости перевести интерфейс в пассивный режим установите флажок **Пассивный интерфейс**. В пассивном режиме интерфейсы не отправляют OSPF hello-пакеты и активно не участвуют в OSPF-маршрутизации. Как правило, в пассивный режим переводятся интерфейсы, которые не нуждаются в обновлениях маршрутной информации, например интерфейсы, подключенные к пользовательским устройствам или сетям, не входящим в OSPF-домен.

13. При необходимости использовать протокол BFD для обнаружения потери связности установите флажок **BFD**. По умолчанию флажок снят.

14. При необходимости настройте OSPF-таймеры:

    a. Установите флажок **OSPF-таймеры**. По умолчанию флажок снят.

    b. В поле **Hello-интервал (сек.)** введите интервал времени в секундах для отправки интерфейсом hello-сообщений. Диапазон значений: от 1 до 65 535.

    c. В поле **Dead-интервал (сек.)** введите время в секундах в течение которого интерфейс должен ожидать получения hello-сообщений от OSPF-соседей. Если в течение указанного времени от соседа не поступает hello-сообщений, интерфейс считает его недоступным. Диапазон значений: от 1 до 65 535.

15. В поле **Интервал повторной передачи (сек.)** введите интервал времени в секундах для повторной отправки потерянных пакетов. Диапазон значений от 1 до 65 535.

16. В поле **Задержка при передаче (сек.)** введите время задержки в секундах перед отправкой первого OSPF-пакета. Диапазон значений от 1 до 65 535.

17. Нажмите на кнопку **Сохранить**.

    OSPF-интерфейс будет создан и отобразится в таблице.

18. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание OSPF-интерфейса на всех устройствах, использующих шаблон CPE.

Чтобы создать OSPF-интерфейс на всех устройствах, использующих шаблон CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF** → **OSPF-интерфейсы**.

   Отобразится таблица OSPF-интерфейсов.

4. Нажмите на кнопку **+ Конфигурирование OSPF-интерфейса**.

5. В открывшемся окне в раскрывающемся списке **Интерфейс** выберите ранее созданный сетевой интерфейс, поверх которого требуется создать OSPF-интерфейс.

6. В поле **OSPF-область** введите идентификатор OSPF-области, к которой относится интерфейс, в формате IPv4-адреса или целого числа.

7. При необходимости настройте аутентификацию в OSPF:

   a. В раскрывающемся списке **Аутентификация** выберите метод аутентификации:

      - **Хеш-функция** – использовать MD5-алгоритм, который обеспечивает безопасность взаимодействия за счет подтверждения подлинности пакетов с помощью общего секретного ключа.

      - **Пароль** – использовать незашифрованный пароль. Этот метод аутентификации является менее надежным по сравнению с **Хеш-функция**, однако он может обеспечить аутентификацию при использовании в доверенном сетевом окружении.

   b. Если в раскрывающемся списке **Аутентификация** вы выбрали **Хеш-функция**, в поле **Пароль** введите пароль для аутентификации.

   c. Если в раскрывающемся списке **Аутентификация** вы выбрали **Хеш-функция**, выполните следующие действия:

      1. В поле **Key ID** введите MD5-хеш. Диапазон значений: от 1 до 255.

      2. В поле **Ключ** введите MD5-ключ.

8. В поле **Стоимость** введите метрику интерфейса. Диапазон значений: от 1 до 65 535.

9. В раскрывающемся списке **Тип сети** выберите тип сети, связанной с интерфейсом:

   - **Широковещательная**.

   - **Не широковещательная**.

   - **point-to-multipoint**.

   - **point-to-point**.

10. В поле **Приоритет** введите приоритет интерфейса. Устройство CPE с наивысшим приоритетом интерфейса становится выделенным маршрутизатором (англ. designated router), в то время как устройство со вторым по величине приоритетом становится резервным выделенным маршрутизатором (англ. backup designated router).

11. При необходимости перевести интерфейс в пассивный режим установите флажок **Пассивный интерфейс**. В пассивном режиме интерфейсы не отправляют OSPF hello-пакеты и активно не участвуют в OSPF-маршрутизации. Как правило, в пассивный режим переводятся интерфейсы, которые не нуждаются в обновлениях маршрутной информации, например интерфейсы, подключенные к пользовательским устройствам или сетям, не входящим в OSPF-домен.

12. При необходимости использовать протокол BFD для обнаружения потери связности установите флажок **BFD**. По умолчанию флажок снят.

13. При необходимости настройте OSPF-таймеры:

    a. Установите флажок **OSPF-таймеры**. По умолчанию флажок снят.

    b. В поле **Hello-интервал (сек.)** введите интервал времени в секундах для отправки интерфейсом hello-сообщений. Диапазон значений: от 1 до 65 535.

    c. В поле **Dead-интервал (сек.)** введите время в секундах в течение которого интерфейс должен ожидать получения hello-сообщений от OSPF-соседей. Если в течение указанного времени от соседа не поступает hello-сообщений, интерфейс считает его недоступным. Диапазон значений: от 1 до 65 535.

14. В поле **Интервал повторной передачи (сек.)** введите интервал времени в секундах для повторной отправки потерянных пакетов. Диапазон значений от 1 до 65 535.

15. В поле **Задержка при передаче (сек.)** введите время задержки в секундах перед отправкой первого OSPF-пакета. Диапазон значений от 1 до 65 535.

16. Нажмите на кнопку **Сохранить**.

    OSPF-интерфейс будет создан и отобразится в таблице.

17. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение OSPF-интерфейса

Вы можете изменить OSPF-интерфейс на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию интерфейса.

Чтобы изменить OSPF-интерфейс на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF** → **OSPF-интерфейсы**.

Отобразится таблица OSPF-интерфейсов.

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 **Изменить** рядом с OSPF-интерфейсом.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить OSPF-интерфейс на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF → OSPF-интерфейсы**.

   Отобразится таблица OSPF-интерфейсов.

4. Нажмите на кнопку **Изменить** рядом с OSPF-интерфейсом.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление OSPF-интерфейса

Вы можете удалить OSPF-интерфейс на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные интерфейсы невозможно восстановить.

Чтобы удалить OSPF-интерфейс на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF → OSPF-интерфейсы**.

   Отобразится таблица OSPF-интерфейсов.

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 **Удалить** рядом с OSPF-интерфейсом.

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

   OSPF-интерфейс будет удален и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить OSPF-интерфейс на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **OSPF → OSPF-интерфейсы**.

   Отобразится таблица OSPF-интерфейсов.

4. Нажмите на кнопку **Удалить** рядом с OSPF-интерфейсом.

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

   OSPF-интерфейс будет удален и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Протокол BFD

Kaspersky SD-WAN поддерживает использование протокола BFD (Bidirectional Forwarding Detection) для быстрого (в пределах одной секунды) обнаружения проблем с сетевой связностью на каналах передачи данных и туннелях. При обнаружении проблемы BFD передает информацию о ней с плоскости передачи данных на плоскость управления сетью.

Между BFD-соседями (англ. BFD peers) устанавливается BFD-сессия, в рамках которой они обмениваются контрольными пакетами для обнаружения проблем с сетевой связностью. Если во время работы BFD-сессии возникает проблема с сетевой связностью, происходит разрыв сессии протокола маршрутизации на соответствующем интерфейсе устройства CPE с последующим перестроением таблиц маршрутизации.

Включение и выключение протокола BFD

Вы можете включить или выключить протокол BFD на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. При включении протокола BFD необходимо создать BFD-соседа.

Чтобы включить или выключить протокол BFD на отдельном устройстве CPE:

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

По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Параметры BFD**.

   Отобразится таблица BFD-соседей.

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 **BFD** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено**– это значение выбрано по умолчанию.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы включить или выключить протокол BFD на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Параметры BFD**.

   Отобразится таблица BFD-соседей.

4. В раскрывающемся списке **BFD** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено**– это значение выбрано по умолчанию.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание BFD-соседа

Вы можете создать BFD-соседа на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Для создания BFD-соседа используйте следующие инструкции:

- Создание BFD-соседа на отдельном устройстве CPE.

Чтобы создать BFD-соседа на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Параметры BFD**.

   Отобразится таблица BFD-соседей.

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 **+ BFD-сосед**.

6. В открывшемся окне в поле **Имя** введите имя BFD-соседа. Максимальная длина: 255 символов.

7. В поле **IP-адрес** введите IP-адрес BFD-соседа.

8. В поле **Интервал передачи (мсек.)** введите интервал времени в миллисекундах для отправки контрольных пакетов BFD-соседу. Диапазон значений: от 60 до 10000.

9. В поле **Интервал получения (мсек.)** введите интервал времени в миллисекундах для получения контрольных пакетов от BFD-соседа. Диапазон значений от 60 до 10000.

10. В поле **Множитель** введите множитель интервала времени для отправки контрольных пакетов, указанного в параметрах BFD-соседа. Этот множитель используется для определения времени, по истечении которого BFD-сессия должна быть разорвана, если BFD-сосед перестает отправлять контрольные пакеты. 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, BFD-сессия разрывается по истечении 400 миллисекунд при условии, что устройство CPE не получило ни одного контрольного пакета.

11. Нажмите на кнопку **Создать**.

    BFD-сосед будет создан и отобразится в таблице.

12. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание BFD-соседа на всех устройствах, использующих шаблон CPE.

Чтобы создать BFD-соседа на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BFD**.

   Отобразится таблица BFD-соседей.

4. Нажмите на кнопку **+ BFD-сосед**.

5. В открывшемся окне в поле **Имя** введите имя BFD-соседа. Максимальная длина: 255 символов.

6. В поле **IP-адрес** введите IP-адрес BFD-соседа.

7. В поле **Интервал передачи (мсек.)** введите интервал времени в миллисекундах для отправки контрольных пакетов BFD-соседу. Диапазон значений: от 60 до 10000.

8. В поле **Интервал получения (мсек.)** введите интервал времени в миллисекундах для получения контрольных пакетов от BFD-соседа. Диапазон значений от 60 до 10000.

9. В поле **Множитель** введите множитель интервала времени для отправки контрольных пакетов, указанного в параметрах BFD-соседа. Этот множитель используется для определения времени, по истечении которого BFD-сессия должна быть разорвана, если BFD-сосед перестает отправлять контрольные пакеты. 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, BFD-сессия разрывается по истечении 400 миллисекунд при условии, что устройство CPE не получило ни одного контрольного пакета.

10. Нажмите на кнопку **Создать**.

    BFD-сосед будет создан и отобразится в таблице.

11. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение BFD-соседа

Вы можете изменить BFD-соседа на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию BFD-соседа.

Чтобы изменить BFD-соседа на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BFD**.

   Отобразится таблица BFD-соседей.

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 **Изменить** рядом с BFD-соседом.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить BFD-соседа на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BFD**.

   Отобразится таблица BFD-соседей.

4. Нажмите на кнопку **Изменить** рядом с BFD-соседом.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление BFD-соседа

Вы можете удалить BFD-соседа в конфигурации на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленных BFD-соседей невозможно восстановить.

Чтобы удалить BFD-соседа на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BFD**.

   Отобразится таблица BFD-соседей.

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 **Удалить** рядом с BFD-соседом.

6. В открывшемся окне нажмите на кнопку **Удалить**.

   BFD-сосед будет удален и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить BFD-соседа на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Параметры BFD**.

   Отобразится таблица BFD-соседей.

4. Нажмите на кнопку **Удалить** рядом с BFD-соседом.

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

   BFD-сосед будет удален и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание и удаление статического IPv4-маршрута

Kaspersky SD-WAN поддерживает использование статических IPv4-маршрутов для передачи пакетов трафика между устройствами CPE и другими маршрутизаторами без применения протоколов маршрутизации.

Вы можете создать статический маршрут на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Перед созданием статического IPv4-маршрута требуется создать сетевой интерфейс. Для создания статического маршрута используйте следующие инструкции:

- Создание статического IPv4-маршрута на отдельном устройстве CPE

Чтобы создать статический IPv4-маршрут на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Статические маршруты**.

   Отобразится список статических маршрутов.

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 создания статического маршрута ＋.

6. В раскрывающемся списке **Интерфейс** выберите ранее созданный сетевой интерфейс для отправки пакетов трафика на узел назначения.

7. В поле **Узел назначения** введите IP-адрес узла назначения.

8. В поле **IPv4-маска** введите маску подсети узла назначения.

9. В поле **Шлюз** введите IP-адрес шлюза для маршрутизации трафика.

10. В поле **Метрика** введите метрику маршрута. По умолчанию указано значение `0`.

11. В поле **MTU** введите значение MTU для маршрута.

12. В раскрывающемся списке **Тип** выберите тип маршрута:

    - **unicast** – стандартный маршрут до узла назначения. Это значение выбрано по умолчанию
    - **local** – маршрут, который добавляется в локальную таблицу маршрутизации устройства CPE и используется для IP-адресов локальных узлов назначения.
    - **broadcast** – маршрут который добавляется в локальную таблицу маршрутизации устройства CPE и используется устройствами канального уровня сетевой модели OSI, поддерживающими использование широковещательных адресов.
    - **multicast** – маршрут, который используется для распределения многоадресного трафика.
    - **unreachable** – маршрут до недоступного узла назначения. При передаче по маршруту пакеты отбрасываются с ICMP-сообщением `Host Unreachable`. Локальные отправители получают ошибку `EHOSTUNREACH`.
    - **prohibit** – маршрут до недоступного узла назначения. При передаче по маршруту пакеты отбрасываются с ICMP-сообщением `Communication Administratively Prohibited`. Локальные отправители получают ошибку `EACCES`.
    - **blackhole** – маршрут до недоступного узла назначения. При передаче по маршруту пакеты отбрасываются без отправления сообщений. Локальные пользователи получают ошибку `EINVAL`.

- **anycast** – маршрут до нескольких узлов назначения, которые имеют anycast-адреса. Такие адреса не могут быть использованы как исходные адреса пакетов трафика.

13. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание статического IPv4-маршрута на всех устройствах, использующих шаблон CPE.

Чтобы создать статический IPv4-маршрут на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **Статические маршруты**.

   Отобразится список статических маршрутов.

4. Нажмите на кнопку создания статического маршрута +.

5. В раскрывающемся списке **Интерфейс** выберите ранее созданный сетевой интерфейс для отправки пакетов трафика на узел назначения.

6. В поле **Узел назначения** введите IP-адрес узла назначения.

7. В поле **IPv4-маска** введите маску подсети узла назначения.

8. В поле **Шлюз** введите IP-адрес шлюза для маршрутизации трафика.

9. В поле **Метрика** введите метрику маршрута. По умолчанию указано значение `0`.

10. В поле **MTU** введите значение MTU для маршрута.

11. В раскрывающемся списке **Тип** выберите тип маршрута:

    - **unicast** – стандартный маршрут до узла назначения. Это значение выбрано по умолчанию
    - **local** – маршрут, который добавляется в локальную таблицу маршрутизации устройства CPE и используется для IP-адресов локальных узлов назначения.
    - **broadcast** – маршрут который добавляется в локальную таблицу маршрутизации устройства CPE и используется устройствами канального уровня сетевой модели OSI, поддерживающими использование широковещательных адресов.
    - **multicast** – маршрут, который используется для распределения многоадресного трафика.
    - **unreachable** – маршрут до недоступного узла назначения. При передаче по маршруту пакеты отбрасываются с ICMP-сообщением `Host Unreachable`. Локальные отправители получают ошибку `EHOSTUNREACH`.
    - **prohibit** – маршрут до недоступного узла назначения. При передаче по маршруту пакеты отбрасываются с ICMP-сообщением `Communication Administratively Prohibited`. Локальные отправители получают ошибку `EACCES`.
    - **blackhole** – маршрут до недоступного узла назначения. При передаче по маршруту пакеты отбрасываются без отправления сообщений. Локальные пользователи получают ошибку `EINVAL`.
    - **anycast** – маршрут до нескольких узлов назначения, которые имеют anycast-адреса. Такие адреса не могут быть использованы как исходные адреса пакетов трафика.

12. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

При необходимости вы можете удалить статический маршрут на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные статические маршруты невозможно восстановить. Для удаления статического маршрута используйте следующие инструкции:

- Удаление статического маршрута на отдельном устройстве CPE.

  Чтобы удалить статический IPv4-маршрут на отдельном устройстве CPE:

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

     По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

  2. Нажмите на устройство CPE.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

  3. Выберите вкладку **Статические маршруты**.

     Отобразится список статических маршрутов.

  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 со статическим IPv4-маршрутом.

     Статический маршрут будет удален и перестанет отображаться в списке.

  6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Удаление статического маршрута на всех устройствах, использующих шаблон CPE.

  Чтобы удалить статический IPv4-маршрут на всех устройствах, использующих шаблон CPE:

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

     Отобразится таблица шаблонов CPE.

  2. Нажмите на шаблон CPE.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

  3. Выберите вкладку **Статические маршруты**.

     Отобразится список статических маршрутов.

  4. Нажмите на кнопку удаления — рядом со статическим IPv4-маршрутом.

     Статический маршрут будет удален и перестанет отображаться в списке.

  5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Протокол VRRP

Kaspersky SD-WAN поддерживает установку устройств CPE на площадках для обеспечения высокой доступности этих площадок. Одним из вариантов организации высокой доступности является использование протокола VRRP (Virtual Router Redundancy Protocol). Вы можете настроить VRRP между несколькими устройствами CPE, а также между устройством и сторонним маршрутизатором.

Во время настройки VRRP вам нужно создать экземпляры VRRP (англ. VRRP instances), которые определяют, какие устройства CPE объединяются в виртуальные маршрутизаторы для обеспечения высокой доступности.

При создании каждого экземпляра VRRP указываются общие параметры протокола VRRP, такие как идентификатор VRID (Virtual Router Identifier) виртуального маршрутизатора и виртуальный IP-адрес для сетевого интерфейса устройства CPE.

Экземпляры VRRP могут быть объединены в группы для синхронизации их работы. Таким образом, если в одном из экземпляров VRRP, входящих в группу, произойдет изменение основного VRRP-маршрутизатора, это изменение также происходит во всех остальных экземплярах VRRP в группе.

Включение и выключение протокола VRRP

Вы можете включить или выключить протокол VRRP на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. При включении протокола VRRP необходимо создать экземпляр VRRP.

Чтобы включить или выключить протокол VRRP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP**.

   Отобразится таблица экземпляров VRPP.

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 **VRRP** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы включить или выключить протокол VRRP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP**.

   Отобразится таблица экземпляров VRPP.

4. В раскрывающемся списке **VRRP** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание экземпляра VRRP

Вы можете создать экземпляр VRRP на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Перед созданием экземпляра VRRP требуется создать сетевой интерфейс. Для создания экземпляра VRRP используйте следующие инструкции:

- Создание экземпляра VRRP на отдельном устройстве CPE.

Чтобы создать экземпляр VRRP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **VRRP**.

   Отобразится таблица экземпляров VRPP.

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 **+ Экземпляр VRRP**.

6. В открывшемся окне в поле **Имя** введите имя экземпляра VRRP. Максимальная длина: 16 символов.

7. В поле **VRID** введите идентификатор Virtual Router Identifier для устройства CPE. Вам нужно указать одинаковый VRID для всех устройств, которые вы хотите объединить в виртуальный маршрутизатор. Диапазон значений: от 1 до 255.

8. В раскрывающемся списке **Интерфейс** выберите ранее созданный сетевой интерфейс, которому требуется назначить виртуальный IP-адрес.

9. В поле **VIP** введите виртуальный IP-адрес для сетевого интерфейса. Вам нужно назначить одинаковый виртуальный IP-адрес сетевым интерфейсам всех устройств CPE, которые требуется объединить в виртуальный маршрутизатор.

10. В раскрывающемся списке **Состояние** выберите роль устройства CPE:

    - **Backup** – резервный VRRP-маршрутизатор. Это значение выбрано по умолчанию.
    - **Master** – основной VRRP-маршрутизатор.

11. В поле **Приоритет** введите приоритет VRRP-маршрутизатора. Чем выше значение, введенное в этом поле, тем выше приоритет. При прекращении работы основного VRRP-маршрутизатора его заменяет резервный VRRP-маршрутизатор с наивысшим приоритетом. Если у резервного VRPP-маршрутизатора выше приоритет чем у основного, он также становится основным. Диапазон значений: от 1 до 1000. По умолчанию указано значение `100`.

12. В поле **Интервал оповещения (сек.)** введите интервал времени в секундах для отправки VRRP-объявлений. Диапазон значений: от 1 до 60. По умолчанию указано значение `5`.

13. При необходимости не изменять роль резервного VRRP-маршрутизатора, ставшего основным, даже если прежний основной VRRP-маршрутизатор восстанавливает работу, установите флажок **Оставлять резервным при восстановлении**. По умолчанию флажок снят.

14. При необходимости настройте отправку VRRP-анонсов в виде unicast-сообщений:

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

    b. В поле **IP основного VRRP-маршрутизатора** введите требуемое значение.

c. В поле **IP резервного VRRP-маршрутизатора** введите требуемое значение.

15. При необходимости используйте пароль для аутентификации VRRP-анонсов:

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

    b. В отобразившемся поле введите пароль. Максимальная длина пароля: 16 символов. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра .

16. Нажмите на кнопку **Создать**.

    Экземпляр VRRP будет создан и отобразится в таблице.

17. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Создание экземпляра VRRP на всех устройствах, использующих шаблон CPE.

Чтобы создать экземпляр VRRP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP**.

   Отобразится таблица экземпляров VRPP.

4. Нажмите на кнопку **+ Экземпляр VRRP**.

5. В открывшемся окне в поле **Имя** введите имя экземпляра VRRP. Максимальная длина: 16 символов.

6. В поле **VRID** введите идентификатор Virtual Router Identifier для устройства CPE. Вам нужно указать одинаковый VRID для всех устройств, которые вы хотите объединить в виртуальный маршрутизатор. Диапазон значений: от 1 до 255.

7. В раскрывающемся списке **Интерфейс** выберите ранее созданный сетевой интерфейс, которому требуется назначить виртуальный IP-адрес.

8. В поле **VIP** введите виртуальный IP-адрес для сетевого интерфейса. Вам нужно назначить одинаковый виртуальный IP-адрес сетевым интерфейсам всех устройств CPE, которые требуется объединить в виртуальный маршрутизатор.

9. В раскрывающемся списке **Состояние** выберите роль устройства CPE:

   - **Backup** – резервный VRRP-маршрутизатор. Это значение выбрано по умолчанию.
   - **Master** – основной VRRP-маршрутизатор.

10. В поле **Приоритет** введите приоритет VRRP-маршрутизатора. Чем выше значение, введенное в этом поле, тем выше приоритет. При прекращении работы основного VRRP-маршрутизатора его заменяет резервный VRRP-маршрутизатор с наивысшим приоритетом. Если у резервного VRPP-маршрутизатора выше приоритет чем у основного, он также становится основным. Диапазон значений: от 1 до 1000. По умолчанию указано значение `100`.

11. В поле **Интервал оповещения (сек.)** введите интервал времени в секундах для отправки VRRP-объявлений. Диапазон значений: от 1 до 60. По умолчанию указано значение `5`.

12. При необходимости не изменять роль резервного VRRP-маршрутизатора, ставшего основным, даже если прежний основной VRRP-маршрутизатор восстанавливает работу, установите флажок **Оставлять резервным при восстановлении**. По умолчанию флажок снят.

13. При необходимости настройте отправку VRRP-анонсов в виде unicast-сообщений:

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

    b. В поле **IP основного VRRP-маршрутизатора** введите требуемое значение.

    c. В поле **IP резервного VRRP-маршрутизатора** введите требуемое значение.

14. При необходимости используйте пароль для аутентификации VRRP-анонсов:

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

b. В отобразившемся поле введите пароль. Максимальная длина пароля: 16 символов. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра.

15. Нажмите на кнопку **Создать**.

    Экземпляр VRRP будет создан и отобразится в таблице.

16. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение экземпляра VRRP

Вы можете изменить экземпляр VRRP на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Описание параметров см. в инструкции по созданию экземпляра VRRP.

Чтобы изменить экземпляр VRRP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

3. Выберите вкладку **VRRP**.

   Отобразится таблица экземпляров VRPP.

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 **Изменить** рядом с экземпляром VRRP.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить экземпляр VRRP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

3. Выберите вкладку **VRRP**.

   Отобразится таблица экземпляров VRPP.

4. Нажмите на кнопку **Изменить** рядом с экземпляром VRRP.
5. В открывшемся окне измените требуемые параметры.
6. Нажмите на кнопку **Сохранить**.
7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление экземпляра VRRP

Вы можете удалить экземпляр VRRP на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные экземпляры VRRP невозможно восстановить.

Чтобы удалить экземпляр VRRP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.
2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.
3. Выберите вкладку **VRRP**.

   Отобразится таблица экземпляров VRPP.
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 **Удалить** рядом с экземпляром VRRP.
6. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

   Экземпляр VRRP будет удален и перестанет отображаться в таблице.
7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить экземпляр VRRP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.
2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.
3. Выберите вкладку **VRRP**.

   Отобразится таблица экземпляров VRPP.
4. Нажмите на кнопку **Удалить** рядом с экземпляром VRRP.
5. В открывшемся окне подтверждения нажмите на кнопку **Удалить**.

Экземпляр VRRP будет удален и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание группы экземпляров VRRP

Вы можете создать группу экземпляров VRRP на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Перед созданием группы экземпляров VRRP требуется создать как минимум один экземпляр VRRP.

Чтобы создать группу экземпляров VRRP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP** → **Группы экземпляров VRRP**.

   Отобразится таблица групп экземпляров VRRP.

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 **+ Группа экземпляров VRRP**.

6. В открывшемся окне в поле **Имя** введите имя группы экземпляров VRRP. Максимальная длина: 16 символов. По умолчанию указано значение `1`.

7. В раскрывающемся списке **Экземпляры VRRP** выберите экземпляры, которые требуется добавить в группу.

8. Нажмите на кнопку **Создать**.

   Группа экземпляров VRRP будет создана и отобразится в таблице.

9. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы создать группу экземпляров VRRP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP** → **Группы экземпляров VRRP**.

   Отобразится таблица групп экземпляров VRRP.

4. Нажмите на кнопку **+ Группа экземпляров VRRP**.

5. В открывшемся окне в поле **Имя** введите имя группы экземпляров VRRP. Максимальная длина: 16 символов. По умолчанию указано значение `1`.

6. В раскрывающемся списке **Экземпляры VRRP** выберите экземпляры, которые требуется добавить в группу.

7. Нажмите на кнопку **Создать**.

   Группа экземпляров VRRP будет создана и отобразится в таблице.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Изменение группы экземпляров VRRP

Вы можете изменить группу экземпляров VRRP на отдельном устройстве CPE или на всех устройствах, которые используют шаблон CPE. Описание параметров см. в инструкции по созданию группы экземпляров VRRP.

Чтобы изменить группу экземпляров VRRP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP** → **Группы экземпляров VRRP**.

   Отобразится таблица групп экземпляров VRRP.

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 **Изменить** рядом с группой экземпляров VRRP.

6. В открывшемся окне измените требуемые параметры.

7. Нажмите на кнопку **Сохранить**.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы изменить группу экземпляров VRRP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP** → **Группы экземпляров VRRP**.

   Отобразится таблица групп экземпляров VRRP.

4. Нажмите на кнопку **Изменить** рядом с группой экземпляров VRRP.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Удаление группы экземпляров VRRP

Вы можете удалить группу экземпляров VRRP на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Удаленные группы экземпляров VRRP невозможно восстановить.

Чтобы удалить группу экземпляров VRRP на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP** → **Группы экземпляров VRRP**.

   Отобразится таблица групп экземпляров VRRP.

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 **Удалить** рядом с группой экземпляров VRRP.

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

   Группа экземпляров VRRP будет удалена и перестанет отображаться в таблице.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы удалить группу экземпляров VRRP на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **VRRP** → **Группы экземпляров VRRP**.

   Отобразится таблица групп экземпляров VRRP.

4. Нажмите на кнопку **Удалить** рядом с группой экземпляров VRRP.

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

   Группа экземпляров VRRP будет удалена и перестанет отображаться в таблице.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Просмотр параметров подключения устройства CPE к сети оператора связи

Если устройство CPE подключено к сети оператора связи через модем, вы можете просмотреть параметры подключения на отдельном устройстве.

Чтобы просмотреть параметры подключения к сети оператора связи на устройстве CPE,

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Модемы**.

Отобразится таблица модемов, через которые устройство CPE подключено к сетям операторов связи, а также параметры этих подключений.

Настройка подключения устройства CPE к Syslog-серверу

Syslog-сервер используется для сбора и хранения журналов событий, сгенерированных на устройствах CPE. Вы можете указать параметры подключения к Syslog-серверу на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Для настройки подключения к Syslog-серверу используйте следующие инструкции:

- Настройка подключения к Syslog-серверу на отдельном устройстве CPE.

Чтобы настроить подключение к Syslog-серверу на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Журналы**.

   Отобразятся параметры подключения к Syslog-серверу.

4. Установите флажок **Переопределить**, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры на выбранной вкладке. По умолчанию флажок снят.

5. В поле **Размер файлов журнала (КБ)** введите размер файлов журнала на устройстве CPE в КБ. Диапазон значений: от 64 до 2048. По умолчанию указано значение 64.

6. В поле **IP или FQDN Syslog-сервера** введите требуемое значение.

7. В поле **Порт Syslog-сервера** введите требуемое значение. Диапазон значений: от 0 до 65 353.

8. В раскрывающемся списке **Протокол Syslog-сервера** выберите протокол для передачи файлов журнала на Syslog-сервер:

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

9. В поле **Префикс для журналов** введите сообщение, которое требуется передавать с каждым файлом журнала на Syslog-сервер. Максимальная длина: 256 символов.

10. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Настройка подключения к Syslog-серверу на всех устройствах, использующих шаблон CPE

Чтобы настроить подключение к Syslog-серверу на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Журналы**.

   Отобразятся параметры подключения к Syslog-серверу.

4. В поле **Размер файлов журнала (КБ)** введите размер файлов журнала на устройстве CPE в КБ. Диапазон значений: от 64 до 2048. По умолчанию указано значение 64.

5. В поле **IP или FQDN Syslog-сервера** введите требуемое значение.

6. В поле **Порт Syslog-сервера** введите требуемое значение. Диапазон значений: от 0 до 65 353.

7. В раскрывающемся списке **Протокол Syslog-сервера** выберите протокол для передачи файлов журнала на Syslog-сервер:

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

8. В поле **Префикс для журналов** введите сообщение, которое требуется передавать с каждым файлом журнала на Syslog-сервер. Максимальная длина: 256 символов.

9. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Настройка подключения устройства CPE к NTP-серверу

Вы можете указать параметры подключения к NTP-серверу на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. Для настройки подключения к NTP-серверу используйте следующие инструкции:

- Настройка подключения к NTP-серверу на отдельном устройстве CPE.

Чтобы настроить подключение к NTP-серверу на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **NTP**.

   Отобразятся параметры подключения к NTP-серверу.

4. Установите флажок **Переопределить**, чтобы игнорировать примененный шаблон CPE и получить возможность изменить параметры на выбранной вкладке. По умолчанию флажок снят.

5. Установите флажок **Подключиться к NTP-серверу**, чтобы разрешить устройству CPE подключаться к NTP-серверу. По умолчанию флажок установлен.

6. Добавьте NTP-сервер:

   a. В блоке **NTP-серверы** введите IP-адрес или FQDN NTP-сервера. Пример значения: `server 0.pool.ntp.org`.

   b. Нажмите на кнопку **+ Добавить**.

   Вы можете добавить несколько серверов.

7. При необходимости использовать устройство CPE в качестве NTP-сервера установите флажок **Использовать как NTP-сервер**. По умолчанию флажок снят.

8. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Настройка подключения к NTP-серверу на всех устройствах, использующих шаблон CPE.

Чтобы настроить подключение к NTP-серверу на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **NTP**.

   Отобразятся параметры подключения к NTP-серверу.

4. Установите флажок **Подключиться к NTP-серверу**, чтобы разрешить устройству CPE подключаться к NTP-серверу. По умолчанию флажок установлен.

5. Добавьте NTP-сервер:

   a. В блоке **NTP-серверы** введите IP-адрес или FQDN NTP-сервера. Пример значения: `server 0.pool.ntp.org`.

   b. Нажмите на кнопку **+ Добавить**.

   Вы можете добавить несколько серверов.

6. При необходимости использовать устройство CPE в качестве NTP-сервера установите флажок **Использовать как NTP-сервер**. По умолчанию флажок снят.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Прошивки

Kaspersky SD-WAN поддерживает обновление прошивок (англ. firmware) на устройствах CPE. Перед установкой новой версии прошивки ее необходимо загрузить в веб-интерфейс оркестратора.

Прошивки распространяются в виде архивов в формате TAR.GZ. Каждый такой архив содержит саму прошивку, а также файл с метаданными в формате YML. Параметры, указанные в файле с метаданными, импортируются в веб-интерфейс оркестратора при загрузке архива с прошивкой.

Если версия прошивки на устройстве CPE устарела по сравнению с одной из добавленных прошивок, имя этой версии подсвечивается оранжевым цветом в столбце **Версия ПО** таблицы, которая отображается в подразделе **Устройства CPE**. Для поиска устройств с устаревшей версией прошивки также можно использовать фильтр **Необходимо обновление**.

При обновлении прошивки вы создаете соответствующую отложенную задачу в планировщике задач. В параметрах задачи можно указать время ее выполнения и включить сброс конфигурации на задействованных устройствах – тогда после установки новой версии прошивки параметры каждого устройства сбрасываются до заводских значений.

Вы также можете настроить принудительную установку прошивки. В этом случае прошивка устанавливается, даже если внутренняя проверка на устройстве CPE выявляет несовместимость его текущей прошивки с новой. Если прошивка задействована в одной из созданных отложенных задач, эту прошивку невозможно удалить.

В процессе обновления прошивки устройство CPE перезагружается.

Загрузка прошивки

Чтобы загрузить прошивку:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Вверху страницы нажмите на кнопку **+ Прошивка**.

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

   Откроется подраздел **Прошивка**, в котором отображается таблица прошивок. Прошивка будет загружена и отобразится в таблице. Параметры прошивки, например дата ее выпуска и совместимая модель устройства CPE, экспортируются из файла с метаданными.

Поиск устройств CPE с устаревшей прошивкой

Чтобы найти устройства CPE с устаревшей прошивкой:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Выполните одно из следующих действий:

   - Найдите устройства CPE с устаревшей прошивкой в столбце **Версия ПО**. Имена устаревших версий подсвечиваются оранжевым цветом.

   - Вверху страницы нажмите на кнопку **Необходимо обновление**, чтобы отобразить список устройств CPE с устаревшей прошивкой.

Обновление прошивки

Вы можете обновить прошивку на выбранных вручную устройствах или на устройствах, которые были сгруппированы с помощью тега. Перед обновлением прошивки ее требуется загрузить в веб-интерфейс оркестратора. В результате обновления прошивки в планировщике задач создается соответствующая отложенная задача.

Для обновления прошивки используйте следующие инструкции:

- Обновление прошивки на устройствах CPE, выбранных вручную.

  Чтобы обновить прошивку на устройствах, выбранных вручную:

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

     По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

  2. Установите флажки рядом с устройствами CPE, на которых требуется обновить прошивку.

  3. Вверху страницы в раскрывающемся списке **Действия** выберите **Обновить прошивку**.

  4. В открывшемся окне в поле **Имя** введите имя отложенной задачи.

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

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

  7. При необходимость сохранить конфигурацию устройства CPE после обновления прошивки установите флажок **Сохранить конфигурацию**. Когда флажок снят, после установки прошивки параметры устройства сбрасываются до заводских значений. По умолчанию флажок установлен.

  8. При необходимости установить 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 два списка. Прошивка устройств CPE из списка сверху будет обновлена, в то время как прошивка устройств из списка снизу обновлена не будет. Вы можете переносить устройства из одного списка в другой.

  10. Нажмите на кнопку **Запланировать**.

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

- Обновление прошивки на устройствах CPE, которым назначен одинаковый тег.

Чтобы обновить прошивку на устройствах CPE, которым назначен одинаковый тег:

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 **Отложенное обновление прошивки**.

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

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

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

7. При необходимость сохранить конфигурацию устройства CPE после обновления прошивки установите флажок **Сохранить конфигурацию**. Когда флажок снят, после установки прошивки параметры устройства сбрасываются до заводских значений. По умолчанию флажок установлен.

8. При необходимости установить 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 требуется обновить прошивку.

10. Нажмите на кнопку **Далее**.

    Отобразятся два списка. Прошивка устройств CPE из списка сверху будет обновлена, в то время как прошивка устройств из списка снизу обновлена не будет. Вы можете переносить устройства из одного списка в другой.

11. Нажмите на кнопку **Создать**.

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

Удаление прошивки

Вы не можете удалить прошивку, которая используется в отложенной задаче. Удаленные прошивки невозможно восстановить.

Чтобы удалить прошивку:

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

   Отобразится таблица прошивок.

2. Установите флажок рядом с прошивкой.

3. Вверху страницы в раскрывающемся списке **Действия** выберите **Удалить**.

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

Прошивка будет удалена и перестанет отображаться в таблице.

Мониторинг компонентов решения

Мониторинг VNF, PNF и устройств CPE обеспечивается внешней системой мониторинга Zabbix. При этом часть данных собирается через контроллер SD-WAN. Для интеграции с системой мониторинга вам нужно развернуть сервер Zabbix в одном из ваших центров обработки данных, либо подключить уже имеющийся сервер.

Сервер Zabbix содержит параметры мониторинга, обрабатывает результаты мониторинга и предоставляет их в виде данных для визуализации, а также отправляет уведомления о возникших ошибках.

Для сбора результатов мониторинга в отдельных центрах обработки данных и их отправки на центральный сервер Zabbix вам нужно развернуть *серверы Zabbix-прокси*. Использование этих серверов снижает нагрузку с ЦПУ сервера Zabbix, уменьшает значение показателя IOPS (Input/Output Operations Per Second) на его диске, а также предоставляет возможность быстрого масштабирования системы мониторинга.

Мониторинг может осуществляться двумя способами в зависимости от программного обеспечения, установленного на оборудовании:

- Если программное обеспечение, установленное на оборудовании, поддерживает установку Zabbix-агентов, оно автоматически передает данные мониторинга серверу Zabbix или Zabbix-прокси.
- Если программное обеспечение, установленное на оборудовании, не поддерживает установку Zabbix-агентов, сервер Zabbix-прокси автоматически подключается к нему через протокол SNMP и собирает необходимые данные.

При управлении устройствами CPE, а также VNF и PNF оркестратор использует API, чтобы автоматически создавать, обновлять и удалять соответствующие им хосты на сервере Zabbix.

Результаты мониторинга отображаются в виде графиков, количество которых зависит от шаблона Zabbix, примененного к компоненту решения. Настройка шаблонов Zabbix мониторинга осуществляется на сервере Zabbix.

Если вы создали шаблон Zabbix для мониторинга отдельной VNF, вам нужно указать его имя в VNF-дескрипторе. После этого вы можете просматривать результаты мониторинга на отдельных VNF. Мониторинг VNF необходим для использования функций Auto-Healing и Auto-Scaling.

Более подробную информацию о настройке системы мониторинга можно получить из официальной документации решения Zabbix.

Подключение к серверу Zabbix

Интеграция с Zabbix обеспечивает мониторинг компонентов решения. Перед подключением к серверу Zabbix его необходимо развернуть его в одном из ваших центров обработки данных.

Чтобы подключиться к серверу 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 по этому 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 к Zabbix API. Вам нужно ввести имя пользователя для учетной записи, имеющей права на чтение и запись в группах узлов сети, которые вы создали на сервере Zabbix для мониторинга компонентов решения Kaspersky SD-WAN. Эта учетная запись используется для аутентификации на сервере Zabbix при отправке API-запроса.

4. В поле **Пароль** введите пароль пользователя для подключения к Zabbix API.

5. В поле **VNF/PNF-группа** введите имя группы узлов сети, которую вы создали на сервере Zabbix для мониторинга VNF или PNF. Если вы не создали группу, оркестратор создает ее автоматически.

6. В поле **Группа CPE** введите имя группы узлов сети, которую вы создали на сервере Zabbix для мониторинга устройств CPE. Если вы не создали группу, оркестратор создает ее автоматически.

7. В поле **Синхронизация триггеров (сек.)** введите интервал времени в секундах для отправки уведомлений о возникших ошибках с сервера Zabbix. Диапазон значений: от 5 до 600. По умолчанию указано значение `600`.

8. Снизу от поля **Токен** нажмите на кнопку **Сгенерировать**, чтобы сгенерировать токен, который сервер Zabbix использует для установки безопасного соединения с оркестратором. Безопасность также обеспечивается TLS-сертификатами. Вы можете ввести токен вручную, а также просмотреть его, нажав на кнопку просмотра 👁.

9. При необходимости проверить доступность сервера Zabbix нажмите на кнопку **Проверить соединение**.

10. Нажмите на кнопку **Применить**.

Подключение к серверу Zabbix-прокси

Интеграция с Zabbix обеспечивает мониторинг компонентов решения. Перед подключением к серверу Zabbix-прокси его необходимо развернуть его в одном из ваших центров обработки данных.

Чтобы подключиться к серверу Zabbix-прокси:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. В панели **Ресурсы** выберите вкладку **Центр обработки данных**.

   Отобразится список центров обработки данных.

3. Нажмите на центр обработки данных, в котором развернут сервер Zabbix-прокси.

4. Выберите вкладку **Системные ресурсы**.

   Отобразятся параметры подключения к серверу Zabbix-прокси.

5. В блоке **Zabbix-прокси** в поле **Имя** введите имя сервера Zabbix-прокси. Введенное имя должно совпадать с именем, указанным в параметрах сервера Zabbix-прокси.

6. В поле **IP** введите IP-адрес сервера Zabbix-прокси.

7. Нажмите на кнопку **Применить**.

Настройка мониторинга устройств CPE

Вам нужно указать параметры мониторинга в конфигурации шаблона CPE и применить этот шаблон к устройствам, на которых требуется просмотреть результаты мониторинга.

Чтобы настроить мониторинг устройств CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Мониторинг**.

   Отобразятся параметры мониторинга устройства CPE.

4. В раскрывающемся списке **Тип мониторинга** выберите одно из следующих значений:

   - **SNMP** – для мониторинга устройств CPE, программное обеспечение которых не поддерживает установку Zabbix-агентов.
   - **Agent** – для мониторинга устройств CPE, программное обеспечение которых поддерживает установку Zabbix-агентов.

5. В поле **Шаблон Zabbix** введите имя шаблона Zabbix.

6. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Просмотр результатов мониторинга

Вы можете просмотреть результаты мониторинга компонентов решения. Для этого используйте следующие инструкции:

- Просмотр результатов мониторинга устройства CPE.

Перед просмотром результатов мониторинга устройства CPE требуется настроить мониторинг в шаблоне CPE.

Чтобы просмотреть результаты мониторинга устройства CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Мониторинг**.

   Отобразятся результаты мониторинга за весь период. Вы можете отобразить результаты за требуемый период с помощью фильтра вверху страницы. Например, вы можете отобразить результаты за год, за месяц или за произвольно заданный временной интервал.

4. Выберите параметр, для которого требуется отобразить результаты мониторинга.

Доступные результаты мониторинга отобразятся в виде графика.

- Просмотр результатов мониторинга экземпляра SD-WAN.

Чтобы просмотреть результаты мониторинга экземпляра SD-WAN:

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

   Отобразится таблица экземпляров SD-WAN.

2. Нажмите на экземпляр SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

3. Выберите вкладку **Мониторинг**.

   Отобразятся результаты мониторинга за весь период. Вы можете отобразить результаты за требуемый период с помощью фильтра вверху страницы. Например, вы можете отобразить результаты за год, за месяц или за произвольно заданный временной интервал.

4. Выберите параметр, для которого требуется отобразить результаты мониторинга.

Доступные результаты мониторинга отобразятся в виде графика.

- Просмотр результатов мониторинга VNF.

Чтобы просмотреть результаты мониторинга VNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Мониторинг**.

   Отобразятся результаты мониторинга за весь период. Вы можете отобразить результаты за требуемый период с помощью фильтра вверху страницы. Например, вы можете отобразить результаты за год, за месяц или за произвольно заданный временной интервал.

5. Выберите параметр, для которого требуется отобразить результаты мониторинга.

Доступные результаты мониторинга отобразятся в виде графика.

- Просмотр результатов мониторинга PNF.

Чтобы просмотреть результаты мониторинга PNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на PNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете PNF.

4. Выберите вкладку **Мониторинг**.

   Отобразятся результаты мониторинга за весь период. Вы можете отобразить результаты за требуемый период с помощью фильтра вверху страницы. Например, вы можете отобразить результаты за год, за месяц или за произвольно заданный временной интервал.

5. Выберите параметр, для которого требуется отобразить результаты мониторинга.

Доступные результаты мониторинга отобразятся в виде графика.

Просмотр ошибок

Система мониторинга присылает вам уведомления об ошибках, которые возникают во время работы компонентов решения. С помощью этих уведомлений вы можете определять и устранять причины неправильной работы компонентов. При возникновении ошибки ей присваивается один из следующих уровней критичности:

- **Предупреждение**.
- **Средний**.
- **Высокий**.
- **Авария**.

Параметры мониторинга, которые вы указываете на сервере Zabbix, определяют, о каких ошибках требуется отправлять уведомления и как эти ошибки классифицируются по уровням критичности. Вы можете просмотреть время возникновения ошибки, а также количество времени, в течение которого она оставалась неисправленной.

Для просмотра ошибок используйте следующие инструкции:

- Просмотр ошибок на устройстве CPE.

  Чтобы просмотреть ошибки на устройстве CPE:

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

     По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

  2. Нажмите на устройство CPE.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

  3. Выберите вкладку **Проблемы**.

     Отобразится таблица ошибок, возникших во время работы устройства CPE.

- Просмотр ошибок на VNF.

Чтобы просмотреть ошибки на VNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на VNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете VNF.

4. Выберите вкладку **Проблемы**.

Отобразится таблица ошибок, возникших во время работы VNF.

- Просмотр ошибок на PNF.

Чтобы просмотреть ошибки на PNF:

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

   Отобразится страница управления сетевыми сервисами.

2. В панели **Сетевые сервисы** выберите сетевой сервис.

   Отобразится графический конструктор с топологией сетевого сервиса.

3. Нажмите на PNF.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

   По умолчанию выбрана вкладка **Варианты развертывания**, на которой отображаются варианты развертывания (англ. flavours) виртуальных машин для сетевой функции. Варианты развертывания описываются в пакете PNF.

4. Выберите вкладку **Проблемы**.

Отобразится таблица ошибок, возникших во время работы PNF.

Включение мониторинга на туннеле

Вы можете включить мониторинг на туннеле. Все туннели, построенные в рамках сети SD-WAN, отображаются в общей таблице туннелей в разделе **Туннели**, а также в графической топологии в разделе **Топология**. В конфигурации устройства CPE на вкладке **Туннели** также отображается таблица туннелей, построенных с использованием этого устройства.

Для включения мониторинга на туннеле используйте следующие инструкции:

- Включение мониторинга на туннеле через общую таблицу.

Чтобы включить мониторинг на туннеле через общую таблицу:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 **Установить пороговые значения**.

5. В открывшемся окне установите флажок **Включить мониторинг пороговых значений туннеля**.

6. При необходимости использовать пороговые значения мониторинга по умолчанию нажмите на кнопку **Параметры по умолчанию**.

7. При необходимости отметить туннель как *нежелательный* и не использовать его при маршрутизации или использовать в последнюю очередь, независимо от качества связи, установите флажок **Нежелательный**. По умолчанию флажок снят.

8. В поле **Интервал обработки ошибок и степени использования (сек.)** введите интервал времени в секундах для измерения количества ошибок на туннеле и уровня его загруженности. Диапазон значений: от 1 до 300. По умолчанию указано значение `60`.

9. Установите флажок **Включить мониторинг ошибок**, чтобы указать пороговое значение количества ошибок на туннеле и в поле **Уровень критических ошибок (ошибок/сек.)** введите требуемое значение. Диапазон значений: от 1 до 1 000 000. По умолчанию флажок снят, а в поле указано значение `1000`.

10. Установите флажок **Включить мониторинг использования**, чтобы указать пороговое значение загруженности туннеля в процентах от установленной скорости сервисного интерфейса и в поле **Критический уровень использования туннеля (%)** введите требуемое значение. По умолчанию флажок снят, а в поле указано значение `95`.

11. В поле **Интервал обработки задержки, джиттера и потери пакетов (сек.)** введите интервал времени в секундах для измерения показателей задержки, джиттера и потери пакетов на туннеле. Диапазон значений: от 1 до 600. По умолчанию указано значение `15`.

12. Установите флажок **Включить мониторинг задержек**, чтобы указать максимальное время задержки в миллисекундах при передаче пакетов по туннелю и в поле **Критический уровень задержек (мс.)** введите требуемое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, а в поле указано значение `100`.

13. Установите флажок **Включить мониторинг джиттера**, чтобы указать максимальное время джиттера в миллисекундах при передаче пакетов по туннелю и в поле **Критический уровень джиттера (мс.)** введите требуемое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, а в поле указано значение `100`.

14. Установите флажок **Включить мониторинг потерь пакетов**, чтобы указать максимальный процент потери пакетов на туннеле и в поле **Критический уровень потерь пакетов (%)** введите требуемое

значение. Диапазон значений: от 1 до 100. По умолчанию флажок снят, а в поле указано значение 2.

15. Сохраните указанные параметры:

    - Нажмите на кнопку **Сохранить**, чтобы сохранить указанные параметры мониторинга на туннеле.

    - Нажмите на кнопку **Сохранить для обоих туннелей**, чтобы сохранить указанные параметры мониторинга на туннеле, а также на аналогичном встречном туннеле.

- Включение мониторинга на туннеле через графическую топологию.

Чтобы включить мониторинг на туннеле через графическую топологию:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 **Установить пороговые значения**.

5. В открывшемся окне установите флажок **Включить мониторинг пороговых значений туннеля**.

6. При необходимости использовать пороговые значения мониторинга по умолчанию нажмите на кнопку **Параметры по умолчанию**.

7. При необходимости отметить туннель как *нежелательный* и не использовать его при маршрутизации или использовать в последнюю очередь, независимо от качества связи, установите флажок **Нежелательный**. По умолчанию флажок снят.

8. В поле **Интервал обработки ошибок и степени использования (сек.)** введите интервал времени в секундах для измерения количества ошибок на туннеле и уровня его загруженности. Диапазон значений: от 1 до 300. По умолчанию указано значение `60`.

9. Установите флажок **Включить мониторинг ошибок**, чтобы указать пороговое значение количества ошибок на туннеле и в поле **Уровень критических ошибок (ошибок/сек.)** введите требуемое значение. Диапазон значений: от 1 до 1 000 000. По умолчанию флажок снят, а в поле указано значение `1000`.

10. Установите флажок **Включить мониторинг использования**, чтобы указать пороговое значение загруженности туннеля в процентах от установленной скорости сервисного интерфейса и в поле **Критический уровень использования туннеля (%)** введите требуемое значение. По умолчанию флажок снят, а в поле указано значение `95`.

11. В поле **Интервал обработки задержки, джиттера и потери пакетов (сек.)** введите интервал времени в секундах для измерения показателей задержки, джиттера и потери пакетов на туннеле. Диапазон значений: от 1 до 600. По умолчанию указано значение `15`.

12. Установите флажок **Включить мониторинг задержек**, чтобы указать максимальное время задержки в миллисекундах при передаче пакетов по туннелю и в поле **Критический уровень задержек (мс.)** введите требуемое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, а в поле указано значение `100`.

13. Установите флажок **Включить мониторинг джиттера**, чтобы указать максимальное время джиттера в миллисекундах при передаче пакетов по туннелю и в поле **Критический уровень джиттера (мс.)** введите требуемое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, а в поле указано значение `100`.

14. Установите флажок **Включить мониторинг потерь пакетов**, чтобы указать максимальный процент потери пакетов на туннеле и в поле **Критический уровень потерь пакетов (%)** введите требуемое значение. Диапазон значений: от 1 до 100. По умолчанию флажок снят, а в поле указано значение `2`.

15. Сохраните указанные параметры:

    - Нажмите на кнопку **Сохранить**, чтобы сохранить указанные параметры мониторинга на туннеле.
    - Нажмите на кнопку **Сохранить для обоих туннелей**, чтобы сохранить указанные параметры мониторинга на туннеле, а также на аналогичном встречном туннеле.

- **Включение мониторинга на туннеле через отдельное устройство CPE**.

Чтобы включить мониторинг на туннеле через отдельное устройство CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Туннели**.

   Отобразится таблица туннелей.

4. Нажмите на кнопку **Управление** рядом с туннелем и в раскрывающемся списке выберите **Установить пороговые значения**.

5. В открывшемся окне установите флажок **Включить мониторинг пороговых значений туннеля**.

6. При необходимости использовать пороговые значения мониторинга по умолчанию нажмите на кнопку **Параметры по умолчанию**.

7. При необходимости отметить туннель как *нежелательный* и не использовать его при маршрутизации или использовать в последнюю очередь, независимо от качества связи, установите флажок **Нежелательный**. По умолчанию флажок снят.

8. В поле **Интервал обработки ошибок и степени использования (сек.)** введите интервал времени в секундах для измерения количества ошибок на туннеле и уровня его загруженности. Диапазон значений: от 1 до 300. По умолчанию указано значение `60`.

9. Установите флажок **Включить мониторинг ошибок**, чтобы указать пороговое значение количества ошибок на туннеле и в поле **Уровень критических ошибок (ошибок/сек.)** введите требуемое значение. Диапазон значений: от 1 до 1 000 000. По умолчанию флажок снят, а в поле указано значение `1000`.

10. Установите флажок **Включить мониторинг использования**, чтобы указать пороговое значение загруженности туннеля в процентах от установленной скорости сервисного интерфейса и в поле **Критический уровень использования туннеля (%)** введите требуемое значение. По умолчанию флажок снят, а в поле указано значение `95`.

11. В поле **Интервал обработки задержки, джиттера и потери пакетов (сек.)** введите интервал времени в секундах для измерения показателей задержки, джиттера и потери пакетов на туннеле. Диапазон значений: от 1 до 600. По умолчанию указано значение `15`.

12. Установите флажок **Включить мониторинг задержек**, чтобы указать максимальное время задержки в миллисекундах при передаче пакетов по туннелю и в поле **Критический уровень задержек (мс.)** введите требуемое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, а в поле указано значение `100`.

13. Установите флажок **Включить мониторинг джиттера**, чтобы указать максимальное время джиттера в миллисекундах при передаче пакетов по туннелю и в поле **Критический уровень джиттера (мс.)** введите требуемое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, а в поле указано значение `100`.

14. Установите флажок **Включить мониторинг потерь пакетов**, чтобы указать максимальный процент потери пакетов на туннеле и в поле **Критический уровень потерь пакетов (%)** введите требуемое значение. Диапазон значений: от 1 до 100. По умолчанию флажок снят, а в поле указано значение `2`.

15. Сохраните указанные параметры:

    - Нажмите на кнопку **Сохранить**, чтобы сохранить указанные параметры мониторинга на туннеле.

    - Нажмите на кнопку **Сохранить для обоих туннелей**, чтобы сохранить указанные параметры мониторинга на туннеле, а также на аналогичном встречном туннеле.

16. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Просмотр состояния решения и его компонентов

Вы можете просматривать информацию о решения и его компонентов в разделе **Обозреватель**, который открывается автоматически после того, как вы аутентифицируетесь в веб-интерфейсе оркестратора.

Чтобы просмотреть состояние компонентов решения,

в меню перейдите в раздел **Обозреватель**.

Отобразятся блоки, между которыми распределена информация. Например, в блоке **Недоступные CPE** отображаются устройства CPE, доступ к которым был потерян. Если компонент решения работает правильно, в соответствующем блоке отображается сообщение *Все работает правильно*.

Блоки можно перетаскивать мышью для изменения порядка их отображения. Вверху каждого блока есть кнопка обновления, при нажатии на которую сбрасывается вся отображаемая информация. Вы также можете использовать кнопку настройки в верхнем углу страницы, чтобы сбросить статистику или изменить интервал обновления информации в блоках.

Протокол SNMP

Вы можете использовать протокол SNMP, чтобы собирать данные мониторинга на оборудовании, не поддерживающем установку Zabbix-агентов. В этом случае вместо Zabbix-агента устанавливается специальная программная сущность – *SNMP-агент*. Он осуществляет постоянный мониторинг оборудования, собирая основную информацию о статусе, показателях производительности, а также конфигурации. Собранная информация затем передается *SNMP-менеджеру*, который является централизованной системой, занимающейся обработкой полученных данных мониторинга. В Kaspersky SD-WAN в роли SNMP-менеджера выступает сервер Zabbix-прокси.

Работа протокола SNMP осуществляется на прикладном уровне TCP/IP (седьмой уровень модели OSI). SNMP-менеджер и SNMP-агенты обмениваются запросами и уведомлениями. В обоих случаях речь идет о стандартных сообщениях. Разница заключается в направлении, в котором отправлено сообщение, а также в его функции.

Когда SNMP-менеджер отправляет SNMP-агенту сообщение, оно используется, чтобы получить данные мониторинга и является *запросом*. По умолчанию SNMP-агенты получают запросы от SNMP-менеджера через порт 161. При этом менеджер может отправлять запросы через любой доступный порт. Ответ приходит на тот же порт, с которого был отправлен запрос.

В то же время если SNMP-агент отправляет SNMP-менеджеру сообщение, оно используется, чтобы предоставить данные мониторинга и является *уведомлением*. По умолчанию SNMP-менеджер получает уведомления от SNMP-агентов через порт 162. При этом агенты могут отправлять уведомления через любые доступные порты. Существует два типа уведомлений:

- *Уведомления-ловушки* (англ. traps) – это уведомления, которые SNMP-агент отправляет без предварительного запроса от SNMP-менеджера, содержащие информацию об определенных событиях. При возникновении указанного вами события, например выключении оборудования или одного из его сетевых интерфейсов, SNMP-агент генерирует уведомление-ловушку и отправляет его SNMP-менеджеру в виде UPD-сообщения. Ловушки позволяют оборудованию автоматически информировать SNMP-менеджер о возникновении важных 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 SNMP-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 приема SNMP-агенту. Механизм подтверждения приема позволяет убедиться в надежности доставки уведомлений.

При использовании протокола TLS или DTLS уведомления-ловушки приходят на порт 10162 SNMP-менеджера, а запросы на информирование – на порт 10161.

В случае SNMP 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.

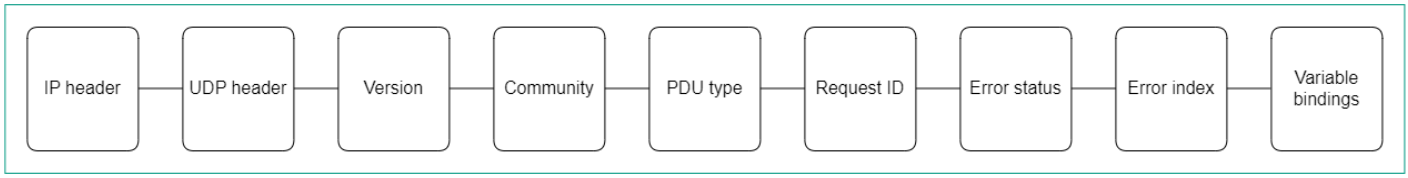


Схема единицы данных протокола SNMP

Настройка подключения SNMP-менеджера к SNMP-агентам

Вам нужно указать параметры подключения SNMP-менеджера к SNMP-агентам, установленным на оборудовании, например на устройствах CPE. В Kaspersky SD-WAN в роли SNMP-менеджера выступает сервер Zabbix-прокси.

Указанные параметры используются для всех SNMP-агентов. Это позволяет сохранить время и избежать необходимости в индивидуальной настройке оборудования. Исключением являются случаи, когда параметры подключения локально перезаписаны на оборудовании.

Чтобы настроить подключение SNMP-менеджера к SNMP-агентам:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **SNMP**.

   Отобразится таблица уведомлений-ловушек.

4. Вверху страницы в блоке **Параметры менеджера** нажмите на кнопку **Изменить**.

5. В открывшемся окне в поле **Адрес** введите IP-адрес или имя хоста оборудования, 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 SNMP-агентам. По умолчанию указано значение `public`, которое предоставляет доступ только для чтения. Мы рекомендуем изменить значение по умолчанию на более безопасную и уникальную строку сообщества, чтобы обеспечить надежность взаимодействия между вашим SNMP-менеджером и SNMP-агентами.

   Вам нужно указать одинаковую строку сообщества как при настройке подключения SNMP-менеджера к SNMP-агентам, так и при создании уведомлений-ловушек.

7. Нажмите на кнопку **Сохранить**.

Создание уведомления-ловушки

Вы можете создать уведомление-ловушку, которое SNMP-агенты будут отправлять SNMP-менеджеру.

Чтобы создать уведомление-ловушку:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 ловушку.

6. В поле **Порт менеджера** введите IP-адрес или имя хоста SNMP-менеджера. В Kaspersky SD-WAN в роли SNMP-менеджера выступает сервер Zabbix-прокси.

7. В поле **Порт менеджера** введите номер порта SNMP-менеджера. 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 SNMP-агентам. По умолчанию указано значение `public`, которое предоставляет доступ только для чтения. Мы рекомендуем изменить значение по

умолчанию на более безопасную и уникальную строку сообщества, чтобы обеспечить надежность взаимодействия между вашим SNMP-менеджером и SNMP-агентами.

> Вам нужно указать одинаковую строку сообщества как при настройке подключения SNMP-менеджера к SNMP-агентам, так и при создании уведомлений-ловушек.

9. В поле **Разрешенные ловушки** нажмите на кнопку **Изменить** и установите следующие флажки, чтобы выбрать, какие уведомления-ловушки SNMP-агенты могут отправлять SNMP-менеджеру:

   - Установите флажок **ifUpNotification**, чтобы SNMP-агент отправлял SNMP-менеджеру уведомление-ловушку, когда один из сетевых интерфейсов оборудования, на котором установлен агент, переходит в активное состояние.
   - Установите флажок **ifDownNotification**, чтобы SNMP-агент отправлял SNMP-менеджеру уведомление-ловушку, когда один из сетевых интерфейсов оборудования, на котором установлен агент, переходит в неактивное состояние.
   - Установите флажок **swUpNotification**, чтобы SNMP-агент отправлял SNMP-менеджеру уведомление-ловушку, когда оборудование, на котором установлен агент, переходит в активное состояние.
   - Установите флажок **swDownNotification**, чтобы SNMP-агент отправлял SNMP-менеджеру уведомление-ловушку, когда оборудование, на котором установлен агент, переходит в неактивное состояние.

   По умолчанию все флажки установлены.

10. Нажмите на кнопку **Назад**, чтобы продолжить указывать параметры.
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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 измените требуемые параметры. Описание параметров см. в инструкции по созданию уведомления-ловушки.

6. Нажмите на кнопку **Сохранить**.

Удаление уведомления-ловушки

Удаленные уведомления-ловушки невозможно восстановить.

Чтобы удалить уведомление-ловушку:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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.

6. Нажмите на кнопку **Сохранить**.

Уведомление-ловушка будет удалено и перестанет отображаться в таблице.

Туннели, сегменты и транспортные пути

Соединение между устройствами CPE обеспечивается туннелями, которые строятся поверх каналов передачи данных. 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 OpenFlow-коммутатора на устройства 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.

Настройка транспортных путей

Вы можете указать параметры транспортных путей на отдельном устройстве CPE, на всех устройствах, использующих шаблон CPE, а также на всех устройствах в сегменте. Для настройки транспортных путей используйте следующие инструкции:

- **Настройка транспортных путей на отдельном устройстве CPE**.

Чтобы настроить транспортные пути на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

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 на всех устройствах, использующих шаблон CPE.

Чтобы настроить транспортные пути на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

- Настройка транспортных путей на всех устройствах в сегменте.

Чтобы настроить транспортные пути на всех устройствах в сегменте:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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. 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 **AUTO** 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 **AUTO**, 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 **AUTO**. 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 **AUTO** 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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. 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. Все туннели, построенные в рамках сети SD-WAN, отображаются в общей таблице туннелей в разделе **Туннели**, а также в графической топологии в разделе **Топология**. В конфигурации устройства CPE на вкладке **Туннели** также отображается таблица туннелей, построенных 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.

     По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

  2. Нажмите на устройство CPE.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

  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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию 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. Все туннели, построенные в рамках сети SD-WAN, отображаются в общей таблице туннелей в разделе **Туннели**, а также в графической топологии в разделе **Топология**. В конфигурации устройства CPE на вкладке **Туннели** также отображается таблица туннелей, построенных 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 через отдельное устройство CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Включение функции Forward Error Correction

Функция *Forward Error Correction* или *прямая коррекция ошибок* (далее также FEC) снижает потери пакетов трафика на каналах связи, 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 туннелях) 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.

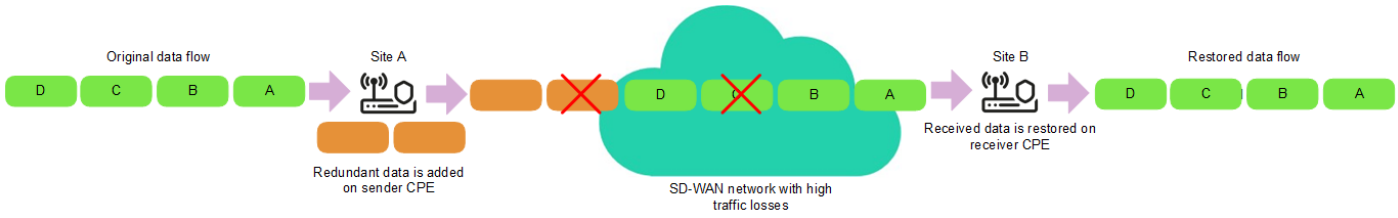


Схема работы функции FEC

Вы можете включить функцию FEC на отдельном туннеле. Все туннели, построенные в рамках сети SD-WAN, отображаются в общей таблице туннелей в разделе **Туннели**, а также в графической топологии в разделе **Топология**. В конфигурации устройства CPE на вкладке **Туннели** также отображается таблица туннелей, построенных 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

  2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

     Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

  2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

     Откроется меню настройки контроллера SD-WAN. 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 устросйтва CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

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.

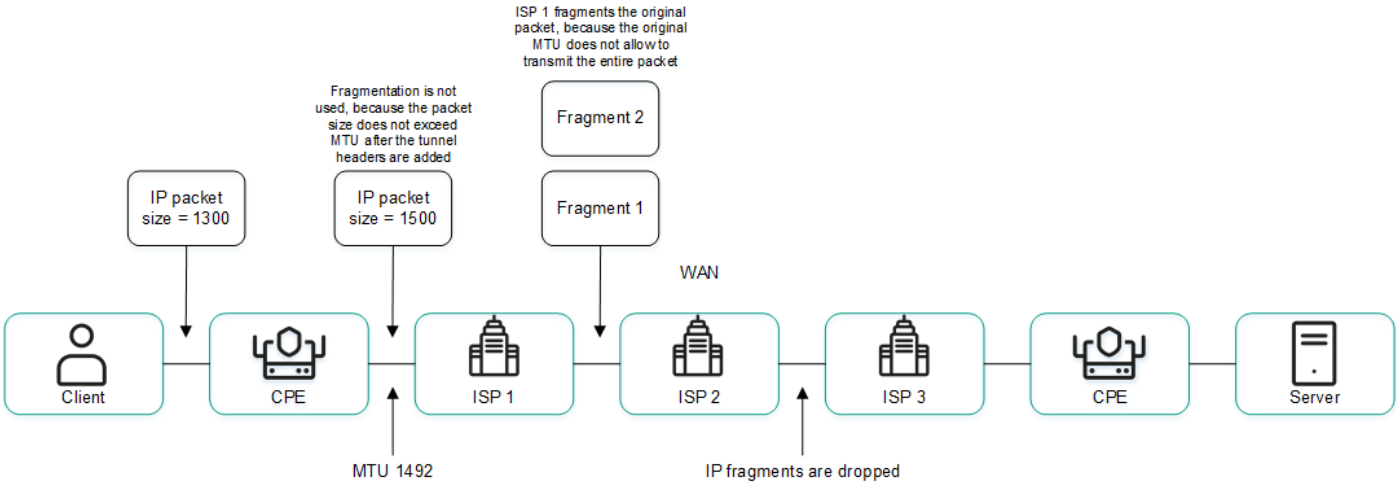
8. Нажмите на кнопку **Сохранить**.

9. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию 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. Все туннели, построенные в рамках сети SD-WAN, отображаются в общей таблице туннелей в разделе **Туннели**, а также в графической топологии в разделе **Топология**. В конфигурации устройства CPE на вкладке **Туннели** также отображается таблица туннелей, построенных 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

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

Фрагментация – это процесс разделения передаваемых по сети пакетов трафика на отдельные части (фрагменты), каждая из которых не превышает размер MTU маршрута. Kaspersky SD-WAN проверяет, поддерживается ли фрагментация пакетов трафика на каждом устройстве CPE.

Размер MTU определяет максимальное количество данных, которые могут быть переданы по сети в составе одного пакета трафика. Проблемы с фрагментацией в рамках сети SD-WAN могут привести к нестабильной передаче данных или ее полной остановке.

Проверка фрагментации пакетов запускается автоматически. При включении каждое устройство CPE отправляет два ICMP-запроса со всех WAN-портов на IP-адреса, которые вы указали при создании интерфейсов SD-WAN либо в файле настройки контроллера SD-WAN при развертывании решения.

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.

Проверка фрагментации пакетов на устройстве CPE может завершиться с одним из следующих результатов:

- *Не поддерживается* – на устройстве невозможна передача фрагментированных пакетов.
- *Неизвестно* – программное обеспечение, установленное на устройстве CPE, не поддерживает проверку возможности фрагментации пакетов.
- *Поддерживается* – на устройстве возможна передача фрагментированных пакетов.

Результат проверки фрагментации отображается в столбце **Фрагментация** общей таблицы туннелей в разделе **Туннели**, а также таблицы туннелей в конфигурации устройства CPE на вкладке **Туннели**. В конфигурации устройства CPE отображаются только туннели, построенные и использованием этого устройства.

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 на отдельном устройстве CPE или на всех устройствах, использующих шаблон CPE. По умолчанию шифрование трафика выключено.

Чтобы включить или выключить шифрование трафика на отдельном устройстве CPE:

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

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Чтобы включить или выключить шифрование трафика на всех устройствах, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Шифрование туннеля**.

   Отобразится политика шифрования трафика.

4. В раскрывающемся списке **Политика шифрования по умолчанию** выберите **Включено** или **Выключено**.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Шифрование трафика на туннеле

Вы можете включить или выключить шифрование трафика на отдельном туннеле. Все туннели, построенные в рамках сети SD-WAN, отображаются в общей таблице туннелей в разделе **Туннели**, а также в графической топологии в разделе **Топология**. В конфигурации устройства CPE на вкладке **Туннели** также отображается таблица туннелей, построенных 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

  2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

     Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию 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

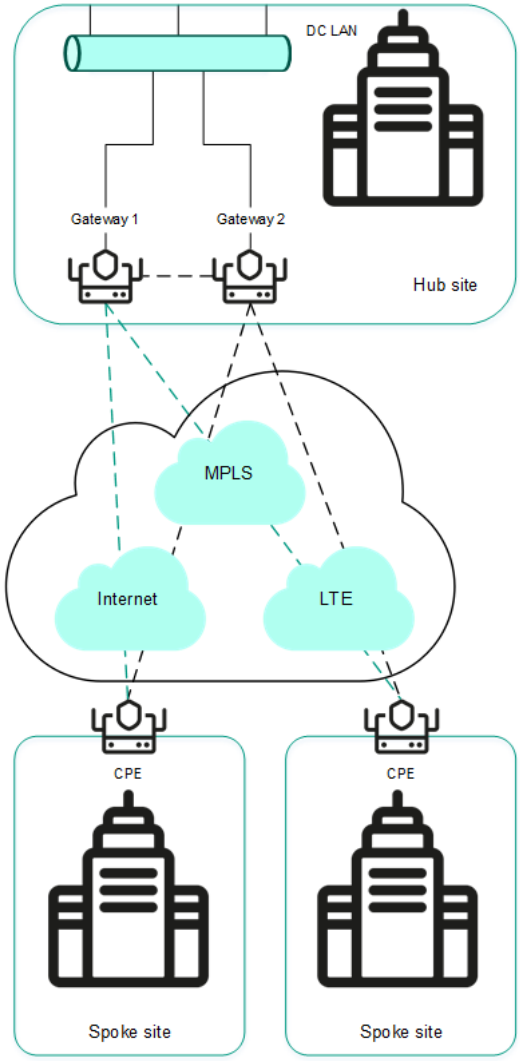
Топология Hub-and-Spoke – это сетевая архитектура, в рамках которой центральная площадка (англ. hub site) подключается к нескольким удаленным площадкам (англ. spoke sites) для обеспечения обмена трафика между ними. Эта топология является наиболее распространенной при построении сетей SD-WAN, так как 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.

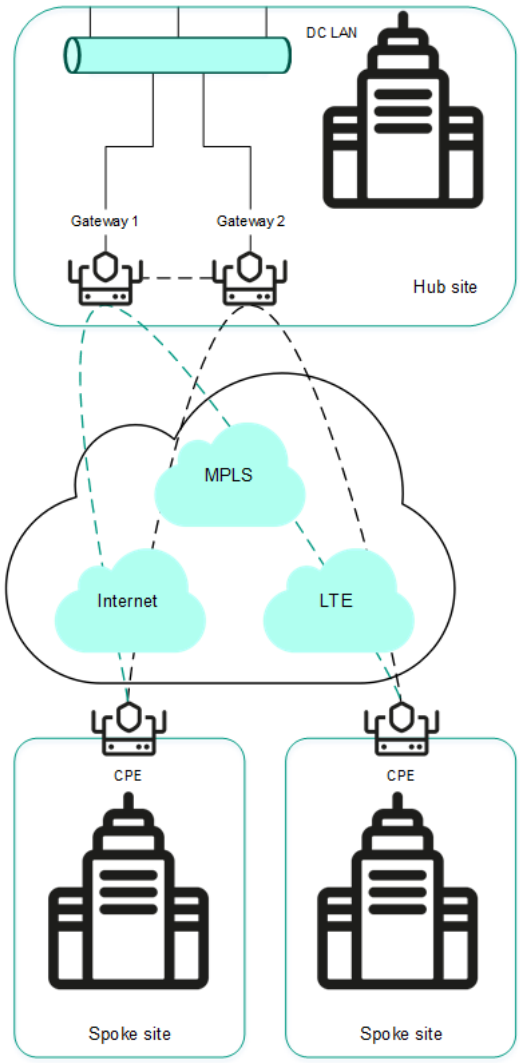
Устройства CPE, регистрирующиеся в оркестраторе, автоматически включаются в управляющий транспортный сервис с ролью Leaf и могут находиться за NAT (Network Address Translation) и PAT (Port Address Translation). В рамках этой топологии невозможна передача трафика напрямую между устройствами.



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.

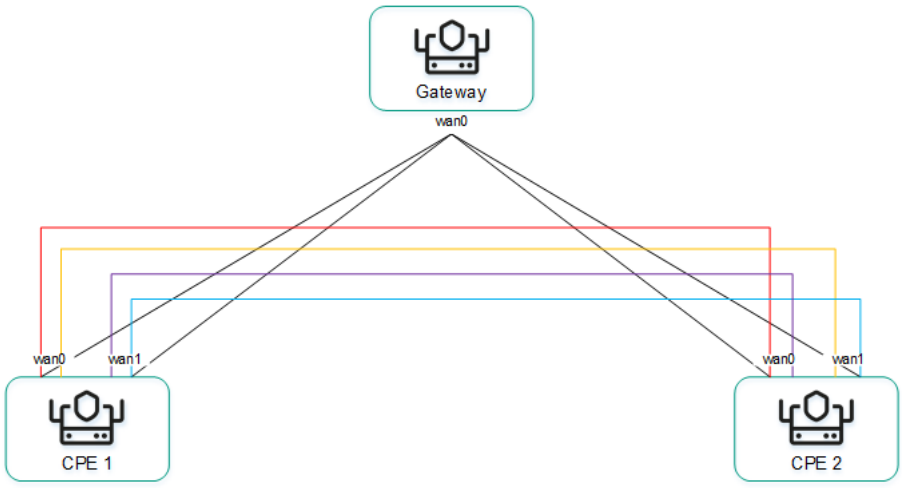
Построение прямых туннелей между устройствами CPE улучшает производительность Kaspersky SD-WAN благодаря следующим свойствам:

- Улучшенные качественные характеристики физического канала передачи данных 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 передачи данных между устройствами CPE, чем в транзитном сценарии CPE1 → шлюз → CPE2.

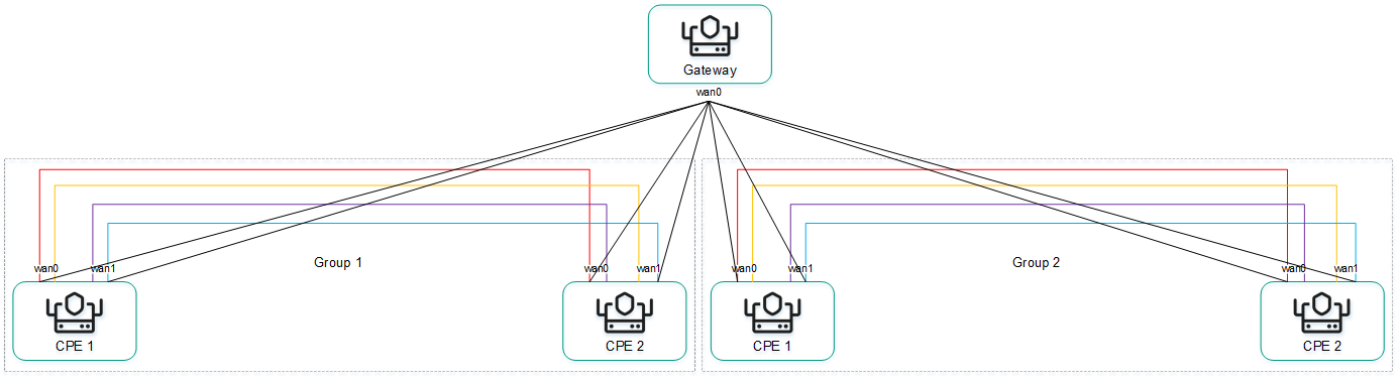
- Сохранение пропускной способности физического канала передачи данных и аппаратных ресурсов шлюза при использовании прямых связей.

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.



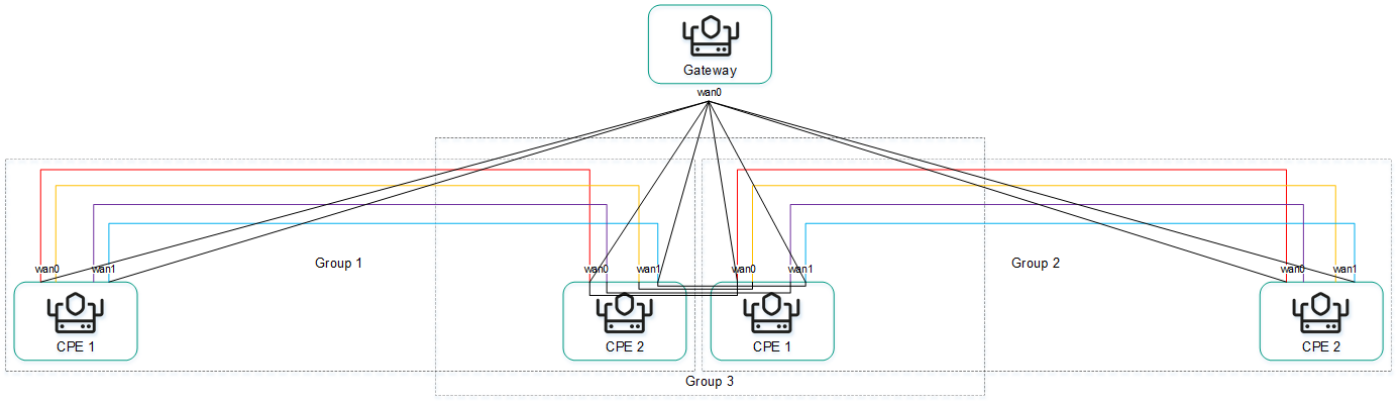
Топология Full-Mesh

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

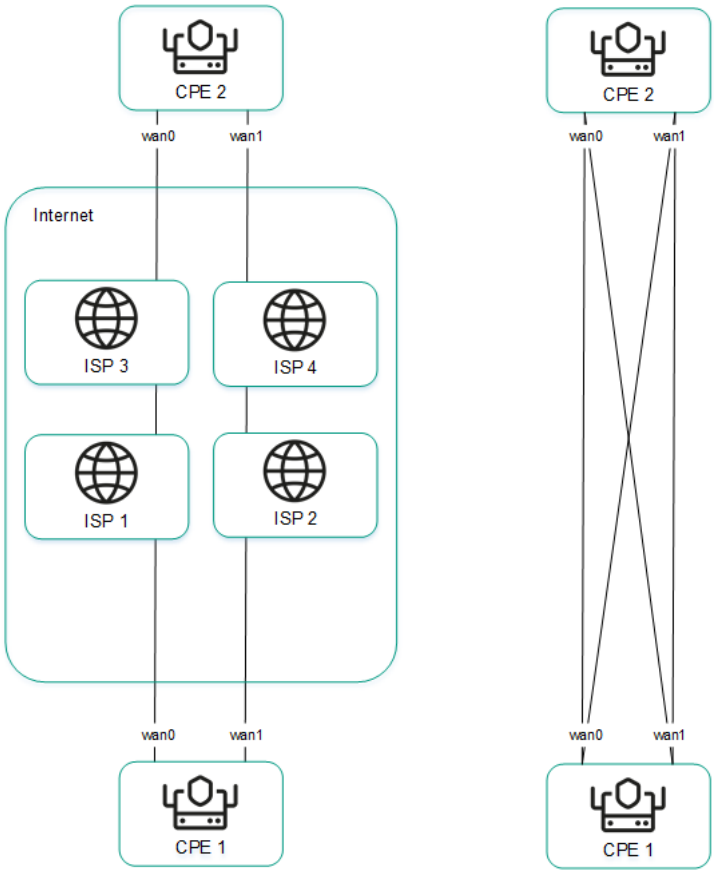
Устройство CPE может входить одновременно в несколько групп, как показано на рисунке ниже.



Топология Partial-Mesh, устройства CPE входят в несколько групп

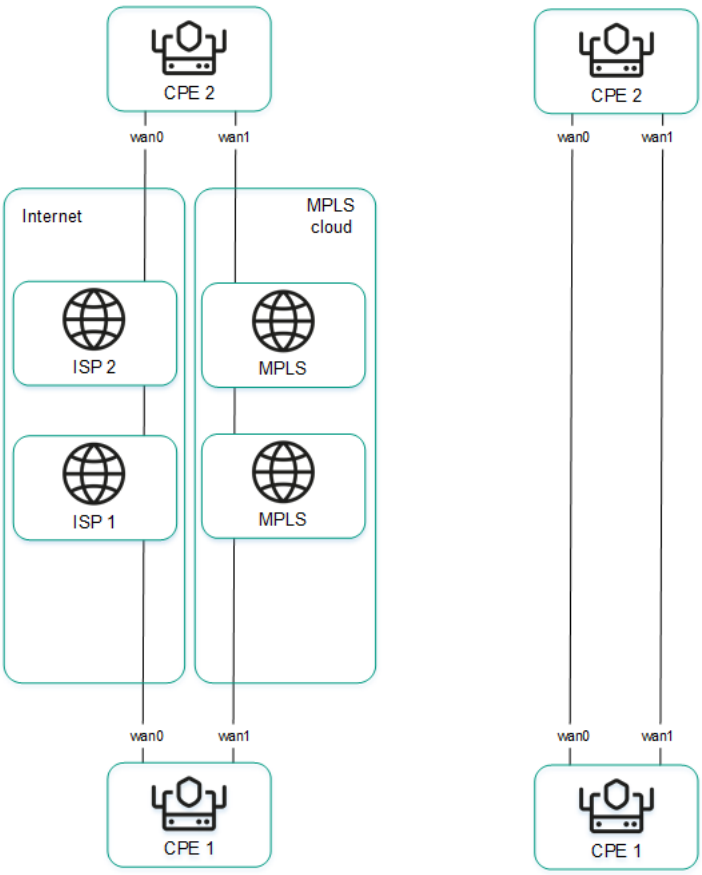
При построении прямых туннелей между устройствами CPE, в зависимости от типа связности устройств через физические каналы, возможны следующие варианты наложенной связности:

- Все физические каналы передачи данных 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 передачи данных 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 отдельному устройству CPE или всем устройствам, использующим шаблон CPE. Для построения топологии Hub-and-Spoke используйте следующие инструкции:

- Назначение роли отдельному устройству CPE.

Чтобы назначить роль отдельному устройству CPE:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 для устройства CPE:

   - **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**.

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

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. В раскрывающемся списке **Роль** выберите роль для устройства CPE:

   - **CPE** – стандартное устройство CPE.
   - **Шлюз** – шлюз SD-WAN.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Назначение роли всем устройствам, использующим шаблон CPE.

Чтобы назначить роль всем устройствам, использующим шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

3. Выберите вкладку **Топология**.

   Отобразятся параметры топологических тегов.

4. В раскрывающемся списке **Роль** выберите роль для связанных с шаблоном CPE устройств:

   - **CPE** – стандартное устройство CPE.
   - **Шлюз** – шлюз SD-WAN.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона 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 отдельному устройству CPE или всем устройствам, использующим шаблон CPE. Для назначения топологических тегов используйте следующие инструкции:

- Назначение топологического тега отдельному устройству CPE.

Чтобы назначить топологический тег отдельному устройству CPE:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Назначение топологического тега всем устройствам, использующим шаблон CPE.

Чтобы назначить топологический тег всем устройствам, использующим шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания .

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

При необходимости вы можете удалить топологический тег отдельного устройства CPE или всех устройств, использующих шаблон CPE. Для удаления топологических тегов используйте следующие инструкции:

- Удаление топологического тега отдельного устройства CPE

Чтобы удалить топологический тег отдельного устройства CPE:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.

   По умолчанию откроется подраздел **Устройства CPE**, в котором отображается таблица устройств CPE.

2. Нажмите на устройство CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

- Удаление топологического тега всех устройств, использующих шаблон CPE

Чтобы удалить топологический тег всех устройств, использующих шаблон CPE:

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

   Отобразится таблица шаблонов CPE.

2. Нажмите на шаблон CPE.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона 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 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 соглашения об уровне обслуживания (англ. Service Level Agreement, далее также SLA) для пропуска клиентского трафика. Поэтому при одновременном подключении к каналам передачи данных 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 подраздел **SD-WAN → Шаблоны экземпляров SD-WAN**.

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Классы трафика**.

   Отобразится таблица классов трафика.

4. Нажмите на кнопку **Изменить**.

5. В открывшемся окне нажмите на кнопку **+ Класс трафика**, чтобы добавить класс трафика.

6. В столбце **Имя** укажите имя для класса трафика.

7. 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.

8. 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.

9. 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**).

10. 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**).

11. В раскрывающемся списке **Класс управляющего трафика** выберите класс, в который требуется помещать управляющий трафик. По умолчанию выбран первый в таблице класс трафика (**Network control**).

12. 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**.

13. Нажмите на кнопку **Ок**.

14. 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 подраздел **SD-WAN** → **Шаблоны экземпляров SD-WAN**.

     Отобразится таблица шаблонов экземпляров SD-WAN.

  2. Нажмите на шаблон экземпляра SD-WAN.

     Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания.

  3. Выберите вкладку **Классы трафика**.

     Отобразится таблица классов трафика.

  4. Нажмите на кнопку **Изменить**.

  5. Открывшемся окне измените требуемые параметры. Описание параметров см. в инструкции по созданию классов трафика в шаблоне экземпляра SD-WAN.

  6. Нажмите на кнопку **Ок**.

  7. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 уже развернутом экземпляре SD-WAN или в шаблоне экземпляра SD-WAN. 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 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

  2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

     Откроется меню настройки контроллера SD-WAN. 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.

- **Создание классификатора трафика в шаблоне экземпляра SD-WAN**.

Чтобы создать классификатор трафика в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

4. Нажмите на кнопку **+ Классификатор**.

5. В открывшемся окне в поле **Имя** введите имя классификатора трафика.

6. 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.

7. 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**.

8. Если в списке **Тип** вы выбрали **Untrust**, в раскрывающемся списке **Класс трафика** выберите класс, в который требуется помещать весь трафик.

9. Нажмите на кнопку **Создать**.

   Классификатор трафика будет создан и отобразится в таблице.

10. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Изменение классификатора трафика

Вы можете изменить классификатор трафика в уже развернутом экземпляре SD-WAN или в шаблоне экземпляра SD-WAN. Описание параметров см. в инструкции по созданию классификатора трафика.

Чтобы изменить классификатор трафика в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.

Чтобы изменить классификатор трафика в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

4. Нажмите на кнопку **Управление** рядом с классификатором трафика и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Удаление классификатора трафика

Вы можете удалить классификатор трафика в уже развернутом экземпляре SD-WAN или в шаблоне экземпляра SD-WAN. Удаленные классификаторы трафика невозможно восстановить.

Чтобы удалить классификатор трафика в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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.

Чтобы удалить классификатор трафика в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **Классификаторы**.

   Отобразится таблица классификаторов трафика.

4. Нажмите на кнопку **Управление** рядом с классификатором трафика и в раскрывающемся списке выберите **Удалить**.

   Классификатор трафика будет удален и перестанет отображаться в таблице.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

QoS-правила

В этом разделе описана настройка QoS-правил.

Создание QoS-правила

Вы можете создать QoS-правило в уже развернутом экземпляре SD-WAN или в шаблоне экземпляра SD-WAN. 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 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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/с** – это значение выбрано по умолчанию.
      - **Мбит/с**.
      - **Гбит/с**.

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.

- Создание QoS-правила в шаблоне экземпляра SD-WAN.

Чтобы создать QoS-правило в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃.

3. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

4. Нажмите на кнопку **+ QoS-правило**.

5. В открывшемся окне в поле **Имя** введите имя QoS-правила.

6. В раскрывающемся списке **Классификатор** выберите ранее созданный классификатор трафика, который требуется использовать в QoS-правиле.

7. 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.

8. 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/с** – это значение выбрано по умолчанию.
      - **Мбит/с**.
      - **Гбит/с**.

   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%.

9. Нажмите на кнопку **Создать**.

QoS-правило будет создано и отобразится в таблице.

10. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Изменение QoS-правила

Вы можете изменить QoS-правило в уже развернутом экземпляре SD-WAN или в шаблоне экземпляра SD-WAN. Описание параметров см. в инструкции по созданию QoS-правила.

Чтобы изменить QoS-правило в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.

Чтобы изменить QoS-правило в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

4. Нажмите на кнопку **Управление** рядом с QoS-правилом и в раскрывающемся списке выберите **Изменить**.

5. В открывшемся окне измените требуемые параметры.

6. Нажмите на кнопку **Сохранить**.

7. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Удаление QoS-правила

Вы можете удалить QoS-правило в уже развернутом экземпляре SD-WAN или в шаблоне экземпляра SD-WAN. Удаленные QoS-правила невозможно восстановить.

Чтобы удалить QoS-правило в уже развернутом экземпляре SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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.

Чтобы удалить QoS-правило в шаблоне экземпляра SD-WAN:

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

   Отобразится таблица шаблонов экземпляров SD-WAN.

2. Нажмите на шаблон экземпляра SD-WAN.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

3. Выберите вкладку **QoS-правила**.

   Отобразится таблица QoS-правил.

4. Нажмите на кнопку **Управление** рядом с QoS-правилом и в раскрывающемся списке выберите **Удалить**.

   QoS-правило будет удалено и перестанет отображаться в таблице.

5. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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).

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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **P2P-сервисы**.

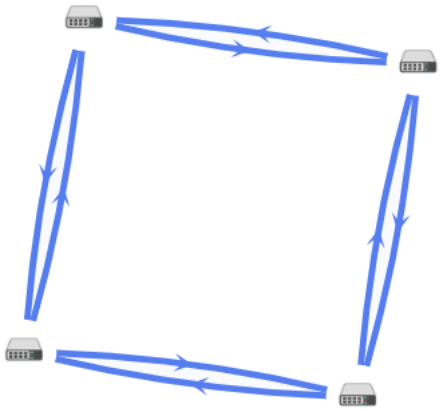
   Отобразится таблица P2P-сервисов.

4. Нажмите на кнопку **Управление** рядом с P2P-сервисом и в раскрывающемся списке выберите **Топология**.

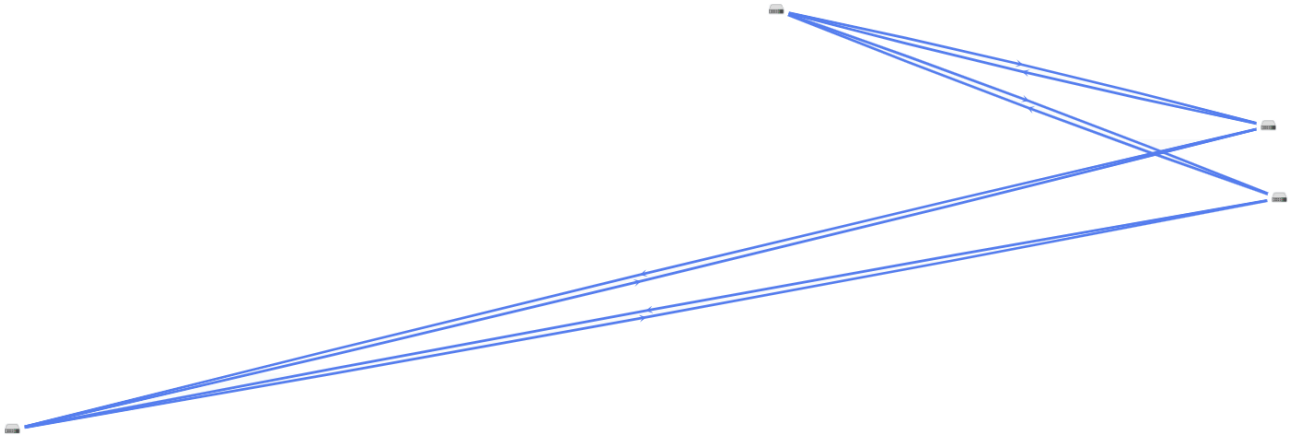
   Откроется окно с топологией P2P-сервиса.

5. При необходимости изменить взаимное расположение устройств CPE в топологии используйте следующие кнопки вверху окна:

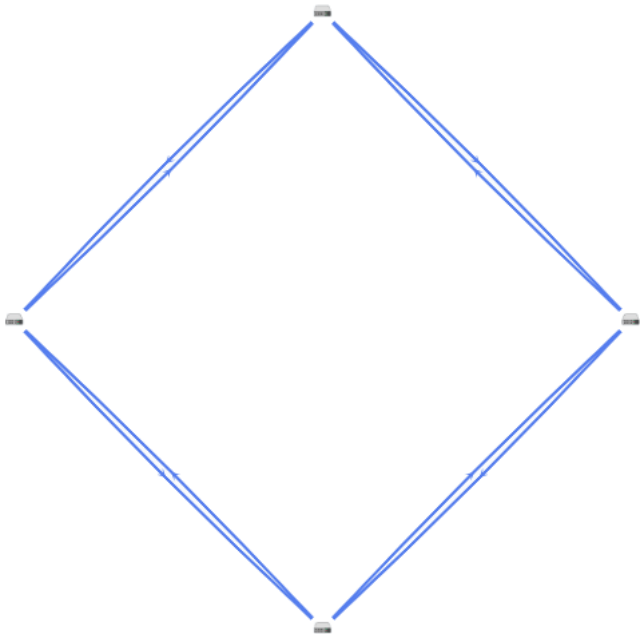
   - **Вручную** – вручную изменить взаимное расположение устройств CPE.
   - **Автоматически** – выбрать одно из значений в раскрывающемся списке, чтобы топология транспортного сервиса была сгенерирована автоматически:
     - **Физическая симуляция** – устройства CPE на схеме располагаются примерно в соответствии с их реальным расположением относительно друг-друга. Например:

     - **Случайно** – устройства CPE располагаются случайным образом. Например:

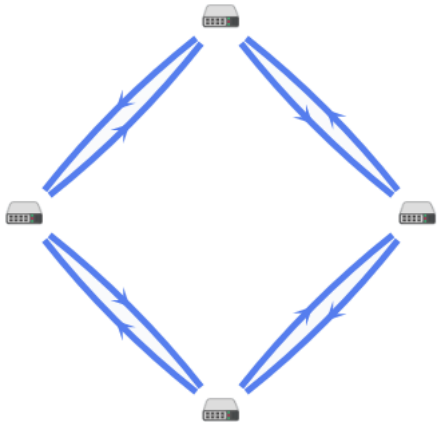
       

     - **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо. Например:



- **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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 требуется применить к серии кадров, когда первый кадр отправляется на контроллер SD-WAN 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 сервисные интерфейсы, добавленные в транспортный сервис, за исключением интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.

- **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отбрасывается.

В обоих случаях при наличии MAC-адреса назначения в таблице MAC-адресов серия кадров отправляется на соответствующий сервисный интерфейс.

9. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице на контроллере SD-WAN. 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 на контроллере SD-WAN:

    - **Flood** – трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано 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 на контроллере SD-WAN. 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, требуется ли использовать Default Forwarding Interface (далее DFI) в транспортном сервисе. Если сервисному интерфейсу назначена роль DFI, на него отправляется весь неизвестный unicast-трафик (англ. unknown unicast). Доступные значения:

    - **Классический** – не использовать DFI. Это значение выбрано 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. Перейдите в раздел **P2M-сервисы**.

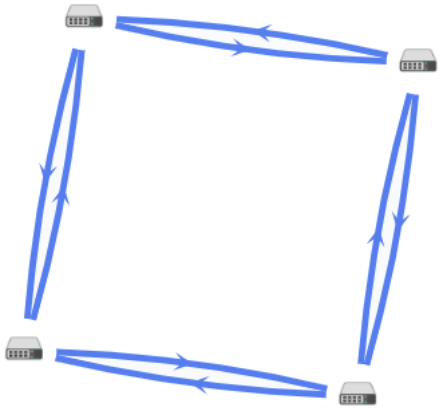
   Отобразится таблица P2M-сервисов.

4. Нажмите на кнопку **Управление** рядом с P2M-сервисом и в раскрывающемся списке выберите **Топология**.

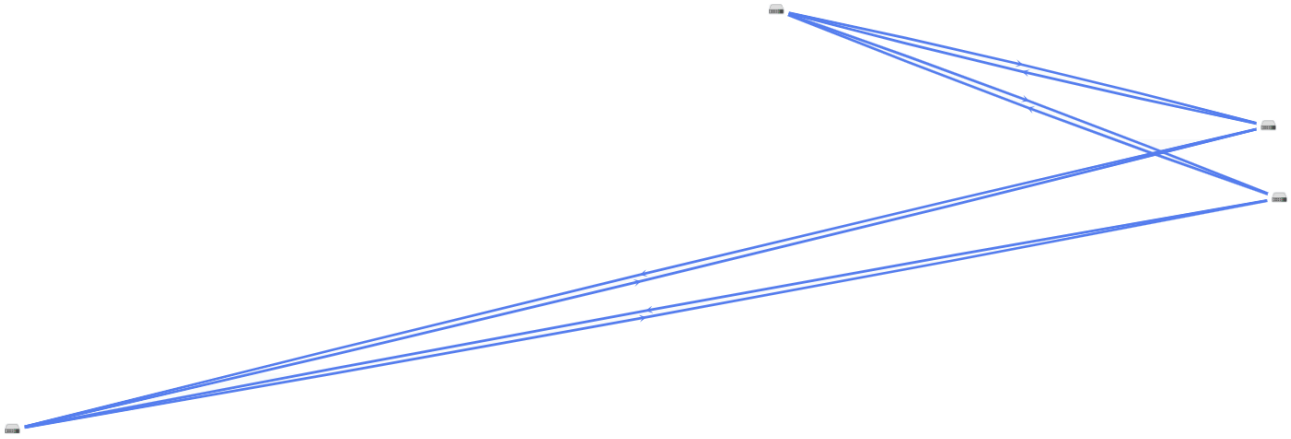
   Откроется окно с топологией P2M-сервиса.

5. При необходимости изменить взаимное расположение устройств CPE в топологии используйте следующие кнопки вверху окна:

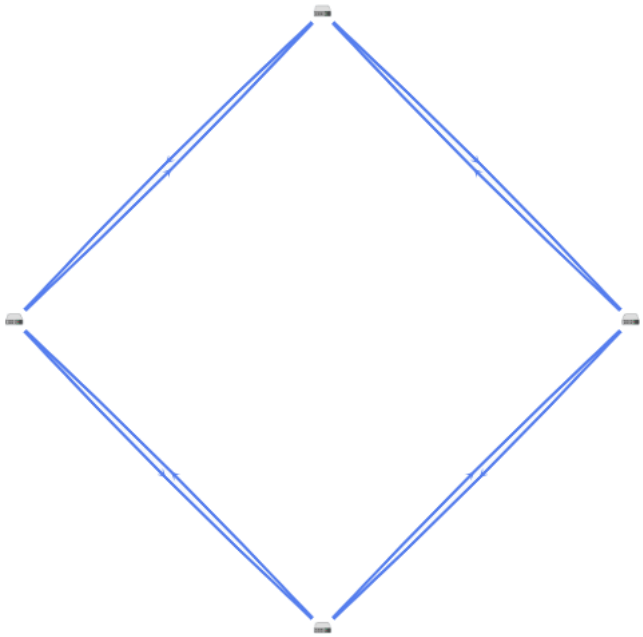
   - **Вручную** – вручную изменить взаимное расположение устройств CPE.
   - **Автоматически** – выбрать одно из значений в раскрывающемся списке, чтобы топология транспортного сервиса была сгенерирована автоматически:
     - **Физическая симуляция** – устройства CPE на схеме располагаются примерно в соответствии с их реальным расположением относительно друг-друга. Например:

     - **Случайно** – устройства CPE располагаются случайным образом. Например:

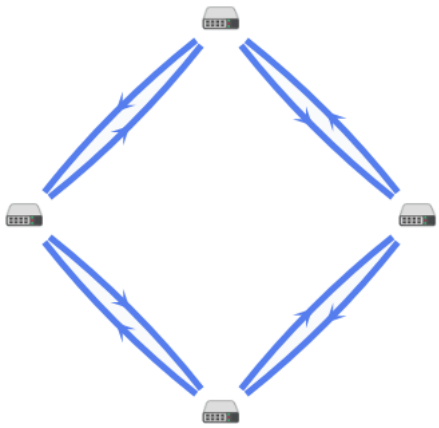


- **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо. Например:



- **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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 требуется применить к серии кадров, когда первый кадр отправляется на контроллер SD-WAN 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 сервисные интерфейсы, добавленные в транспортный сервис, за исключением интерфейса, на который серия кадров пришла изначально. Это значение выбрано по умолчанию.

- **Learn and drop** – контроллер запоминает MAC-адрес источника и проверяет наличие MAC-адреса назначения в таблице MAC-адресов. Если MAC-адрес назначения отсутствует в таблице, серия кадров отбрасывается.

В обоих случаях при наличии MAC-адреса назначения в таблице MAC-адресов серия кадров отправляется на соответствующий сервисный интерфейс.

9. В поле **MAC-возраст (сек.)** введите время в секундах, в течение которого записи хранятся в MAC-таблице на контроллере SD-WAN. 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 на контроллере SD-WAN:

    - **Flood** – трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast). Это значение выбрано 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 на контроллере SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.

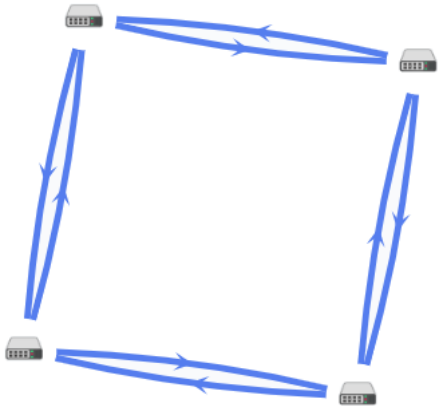
   Откроется окно с топологией M2M-сервиса.

5. При необходимости изменить взаимное расположение устройств CPE в топологии используйте следующие кнопки вверху окна:

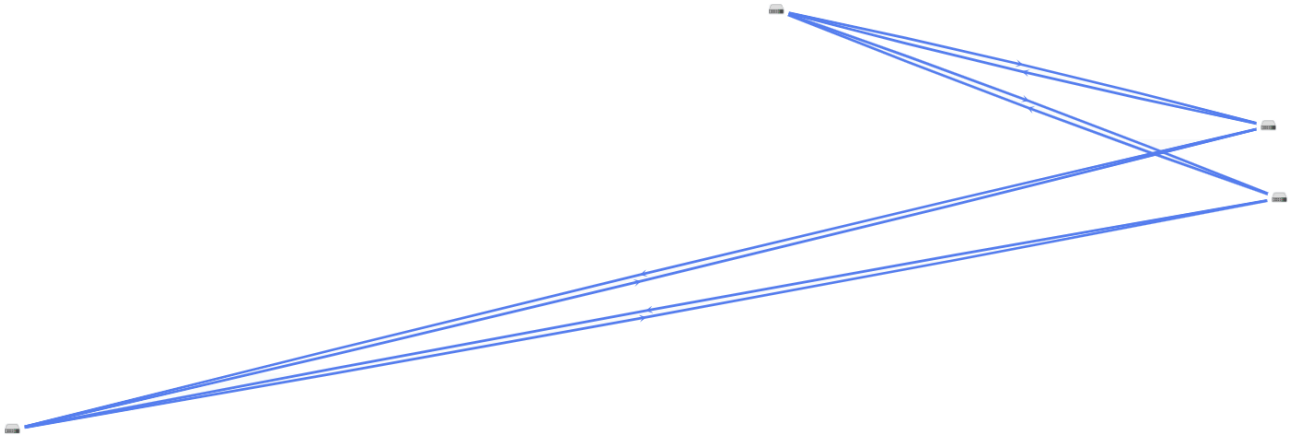
   - **Вручную** – вручную изменить взаимное расположение устройств CPE.

- **Автоматически** – выбрать одно из значений в раскрывающемся списке, чтобы топология транспортного сервиса была сгенерирована автоматически:

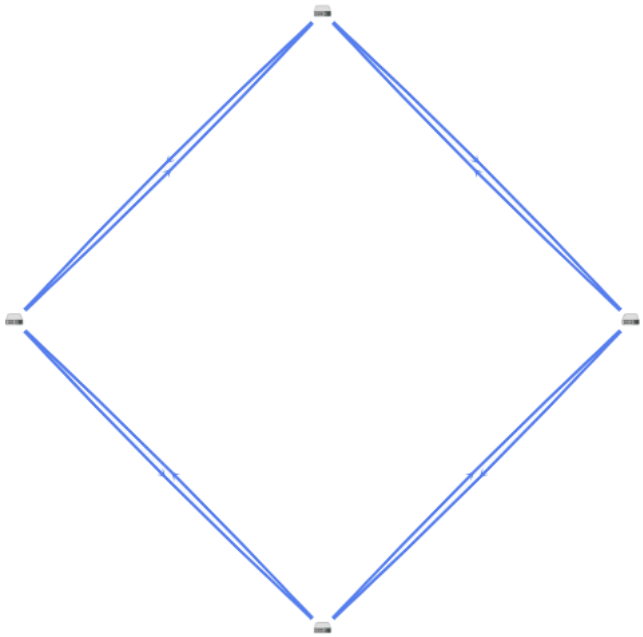
  - **Физическая симуляция** – устройства CPE на схеме располагаются примерно в соответствии с их реальным расположением относительно друг-друга. Например:



  - **Случайно** – устройства CPE располагаются случайным образом. Например:

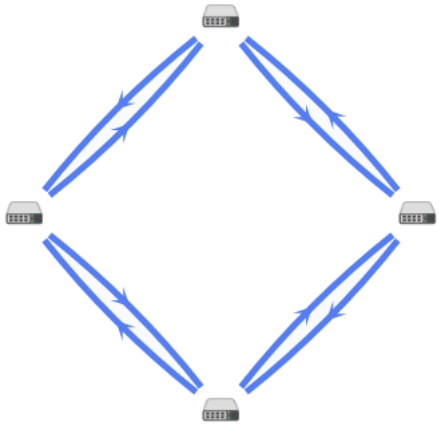


  - **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо. Например:



  - **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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.
2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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.

Добавление транспортного сервиса в шаблоне CPE

Вы можете добавить транспортные сервисы в конфигурации шаблона 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.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

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**.

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. Нажмите на кнопку **Создать**.

    Транспортный сервис будет добавлен и отобразится в таблице.

14. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию 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.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

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 конфигурации шаблона 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.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку развертывания ⌃⌃.

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. Вверху области настройки нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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**.
       - **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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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 инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку 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.

   Внизу страницы отобразится область настройки. Вы можете развернуть область настройки на всю страницу, нажав на кнопку 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.

Настройка контроллера SD-WAN

В этом разделе описаны действия, которые вы можете выполнять с контроллером SD-WAN после развертывания.

Изменение контроллера SD-WAN

Чтобы изменить контроллер SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN, и в раскрывающемся списке выберите **Изменить**.

3. В открывшемся окне измените требуемые параметры.

4. Нажмите на кнопку **Сохранить**.

Перезагрузка контроллера SD-WAN

Некоторые изменения, которые вы вносите в конфигурацию контроллера SD-WAN, требуют его перезагрузки (англ. reprovisioning), чтобы вступить в силу. При перезагрузке свойства контроллера сбрасываются до значений по умолчанию, что может помочь устранить возникающие проблемы и ошибки конфигурации.

Вы также можете перезагрузить контроллер, когда заменяете старое оборудование на новое или обновляете программное обеспечение, чтобы убедиться, что новые функции и улучшения успешно интегрированы в инфраструктуру решения, взаимодействуют с плоскостью управления сетью и готовы к работе.

Чтобы перезагрузить контроллер SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN, и в раскрывающемся списке выберите **Перезагрузить**.

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

Скачивание резервного файла с конфигурацией контроллера SD-WAN

Резервный файл с конфигурацией используется, чтобы восстановить работоспособность контроллера SD-WAN, одинаковым образом настроить контроллеры в разных системных средах и вести учет версий конфигурации на ваших локальных устройствах, чтобы при необходимости вернуться к любой версии.

Наличие резервных файлов также позволяет документировать процесс конфигурации контроллера для последующего анализа внесенных изменений и проведения внутренних аудитов.

Чтобы скачать резервный файл с конфигурацией контроллера SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN, и в раскрывающемся списке выберите **Скачать резервный файл**.

На ваше локальное устройство сохранится файл в формате YAML с конфигурацией контроллера SD-WAN.

Восстановление контроллера SD-WAN

Вы можете восстановить конфигурацию контроллера SD-WAN, используя ранее скачанный резервный файл.

Чтобы восстановить контроллер SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN, и в раскрывающемся списке выберите **Восстановить**.

3. В открывшемся окне укажите путь к файлу с конфигурацией контроллера SD-WAN.

4. Нажмите на кнопку **Восстановить**.

Удаление контроллера SD-WAN

Удаленные контроллеры SD-WAN невозможно восстановить.

Чтобы удалить контроллер SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN, и в раскрывающемся списке выберите **Удалить**.

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

Контроллер SD-WAN будет удален и перестанет отображаться в таблице.

Свойства контроллера SD-WAN

Свойства развернутого контроллера SD-WAN имеют значения по умолчанию. Каждое свойство регулирует работу контроллера, например свойство `controller.listen.port` определяет TCP-интерфейс для входящих соединений, к которому подключаются устройства CPE.

Свойства имеют *методы изменения*, которые определяют, может ли значение отдельного свойства быть изменено и в какой момент изменение вступает в силу. Свойство может иметь следующие методы изменения:

- **Read-only** – свойство напрямую влияет на работу контроллера SD-WAN и не может быть изменено.
- **Reload** – свойство может быть изменено. При изменении значения свойства оркестратор отправляет новое значение в базу данных контроллера SD-WAN. 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 SD-WAN, чтобы сохранить текущее значение.
- **Runtime** – свойство может быть изменено. Новое значение вступает в силу сразу после изменения.

Вы можете изменять свойства с методами изменения Reload и Runtime, сбрасывать их до значений по умолчанию, а также удалять планируемые значения.

Если ваш контроллер SD-WAN развернут в виде кластера из нескольких узлов, вам нужно изменять свойства во время настройки всего кластера. Вы не можете изменять свойства контроллера SD-WAN, когда вы настраиваете один из его узлов.

Изменение и сброс свойств контроллера SD-WAN

Изменения, которые вы вносите в свойства контроллера SD-WAN с методом изменения Runtime, сразу вступают в силу, в то время как свойства с методом изменения Reload требуют перезагрузки контроллера.

Чтобы изменить или сбросить свойства контроллера до значений по умолчанию:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN, и в раскрывающемся списке выберите **Свойства**.

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

3. Выберите вкладку **Изменяемые свойства**.

   Отобразится таблица изменяемых свойств контроллера.

4. При необходимости измените значение отдельного свойства:

   a. Нажмите на кнопку **Управление** рядом со свойством и в раскрывающемся списке выберите **Изменить**.

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

   c. Нажмите на кнопку **Сохранить**.

Если вы изменили свойство с методом изменения Runtime, новое значение отобразится в столбце **Текущее значение**. Новое значение свойства с методом изменения Reload отобразится в столбце **Планируемое значение**.

5. При необходимости сбросьте отдельное свойство до значения по умолчанию:

   a. Нажмите на кнопку **Управление** рядом со свойством и в раскрывающемся списке выберите **Сбросить свойство**.

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

6. При необходимости сбросьте все свойства до значений по умолчанию:

   a. Вверху страницы нажмите на кнопку настройки и в раскрывающемся списке выберите **Сбросить все свойства**.

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

Удаление запланированного значения свойства контроллера SD-WAN

Вам нужно удалить запланированное значение, чтобы отменить изменение свойства контроллера SD-WAN. Это действие применимо только к свойствам с методом изменения Reload.

Чтобы удалить запланированное значение свойства контроллера SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN, и в раскрывающемся списке выберите **Свойства**.

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

3. Выберите вкладку **Изменяемые свойства**.

   Отобразится таблица изменяемых свойств контроллера.

4. При необходимости удалите запланированное значение отдельного свойства:

   a. Нажмите на кнопку **Управление** рядом со свойством и в раскрывающемся списке выберите **Удалить запланированное значение**.

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

5. При необходимости удалите запланированные значения всех свойств:

   a. Вверху страницы нажмите на кнопку настройки и в раскрывающемся списке выберите **Удалить все запланированные значения**.

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

Отдельное запланированное значение или все запланированные значения будут удалены и перестанут отображаться в таблице.

Просмотр информации об узлах контроллера SD-WAN

В меню настройки контроллера SD-WAN отображаются все узлы контроллера SD-WAN – основной и второстепенные (если используются). Вы можете просматривать статистику работы каждого узла, а также таблицу с их свойствами.

Чтобы просмотреть информацию об узлах контроллера SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

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

3. При необходимости просмотреть статистику работы узла, нажмите на кнопку **Управление** рядом с этим узлом и в раскрывающемся списке выберите **Статистика**.

4. При необходимости просмотреть свойства узла, нажмите на кнопку **Управление** рядом с этим узлом и в раскрывающемся списке выберите **Свойства узла**.

Просмотр топологии развернутого экземпляра SD-WAN

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

Обратите внимание на то, что туннель между двумя устройствами CPE можно выбрать и настроить. Например, в топологии экземпляра SD-WAN вы можете указать стоимость туннеля и включить его мониторинг.

Чтобы просмотреть топологию развернутого экземпляра SD-WAN:

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

   Откроется страница управления инфраструктурой сети SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображается таблица контроллеров SD-WAN.

2. Нажмите на кнопку **Управление** рядом с контроллером SD-WAN и в раскрывающемся списке выберите **Меню конфигурации**.

   Откроется меню настройки контроллера SD-WAN. 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. При необходимости настройте топологию:

   - 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 **Внутриполосное управление**, чтобы отобразить топологию динамической маршрутизации трафика, управляющего коммутаторами внутри каналов передачи данных.

  Этот протокол динамической маршрутизации используется только аппаратными SDN-коммутаторами, поэтому установка этого флажка не даст никакого результата при работе с Kaspersky SD-WAN.

- Установите флажок **Имя**, чтобы отобразить имена устройств CPE, используемых в топологии.
- Установите флажок **IP-адрес**, чтобы отобразить IP-адреса устройств CPE, используемых в топологии.

По умолчанию все флажки сняты.

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.

Приложения

В этом разделе содержится информация, которая дополняет основной текст документа.

Руководство по развертыванию демонстрационного стенда Kaspersky SD-WAN в среде VMware

Вы можете получить информацию о развертывании демонстрационного стенда Kaspersky SD-WAN в среде VMware из следующих руководств:

- Руководство по развертыванию демонстрационного стенда Kaspersky SD-WAN в среде VMware, часть 1.
- Руководство по развертыванию демонстрационного стенда Kaspersky SD-WAN в среде VMware, часть 2.

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.

Graceful restart

Функция, которая позволяет устройству CPE уведомить своих соседей о скорой перезагрузке, например при использовании BGP. В этом случае соседи сразу исключают устройство CPE из таблицы маршрутизации, не дожидаясь окончания времени максимального ожидания (англ. timeout).

Physical Network Function (PNF)

Заранее развернутые сетевые функции, которые в готовом виде загружается в веб-интерфейс оркестратора. Оркестратор может осуществлять дальнейшую конфигурацию PNF.

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 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.

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.

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.

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.