kaspersky

Kaspersky SD-WAN

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 2

Содержание

О Kaspersky SD-WAN

Kaspersky SD-WAN используется для построения программно-определяемых распределенных сетей (англ. Software Defined WAN, далее также 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), установленные на клиентских площадках. Управление сетью также может осуществляться через API. Устройства CPE в свою очередь образуют плоскость передачи данных.

Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Инструмент управления, мониторинга и диагностики сети SD-WAN, также отвечающий за виртуализацию сетевых функций (англ. Network Function Virtualization, NFV). Для управления оркестратором используется графический веб-интерфейс.

Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

Решение предназначено для операторов связи (англ. service providers), а также организаций, имеющих крупную филиальную сеть, и используется для замены стандартных маршрутизаторов в распределенных сетях. Процесс развертывания решения не зависит от транспортных технологий, используемых в вашей сети.

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

- Интеллектуальное управление трафиком.
- Автоматическая настройка устройств CPE. Эта функциональность позволяет свести к минимуму необходимость в задействовании специалистов при развертывании устройств на площадках.
- Централизованное управление инфраструктурой сети через веб-интерфейс оркестратора. Например, вы можете использовать веб-интерфейс оркестратора для настройки устройств CPE и туннелей.
- Постоянный мониторинг топологии сети и автоматическое реагирование на ее изменение. Например, вы можете настроить передачу трафика по резервному туннелю в случае обнаружения сбоя в работе основного.
- Автоматическое реагирование сети на изменения качества обслуживания в каналах передачи данных для удовлетворения требований приложений.

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

Схема сети SD-WAN

Поддерживаются следующие каналы передачи данных:

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

Решение также поддерживает использование нескольких туннелей для передачи трафика с учетом требований приложений к пропускной способности и качеству обслуживания.

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

Для функционирования Kaspersky SD-WAN вам нужно убедиться, что ваша сетевая инфраструктура соответствует следующим аппаратным и программным требованиям.

В решение входят следующие программные модули:

- **Оркестратор** – входит в backend-часть решения.

  Инструмент управления, мониторинга и диагностики сети SD-WAN, также отвечающий за виртуализацию сетевых функций (англ. Network Function Virtualization, NFV). Для управления оркестратором используется графический веб-интерфейс.

- Веб-интерфейса оркестратора – входит во frontend-часть решения.

- База данных оркестратора (MongoDB).

- **VNFM**.

  Инструмент конфигурации VNF, развернутых оркестратором.

- Веб-сервер NGINX для балансировки HTTP- и HTTPS-запросов к VNFM и предоставления веб-прокси **устройствам CPE** и **VNF**.

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

  Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

- Резидентная база данных Redis.

- **Контроллер SD-WAN**.

  Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

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 для увеличения общей производительности решения.

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, а также контроллера SD-WAN. Существует два варианта развертывания контроллера:

- В виде VNF – в этом случае используется виртуальная инфраструктура под управлением OpenStack. Узлы контроллера размещаются на вычислительных OpenStack-узлах.

- В виде **PNF** – в этом случае используется отдельная виртуальная машина.

  Заранее развернутая сетевая функция, которая в готовом виде загружается в веб-интерфейс оркестратора. Оркестратор может осуществлять дальнейшую конфигурацию PNF.

Аппаратные требования

Требования к аппаратным ресурсам зависят от количества управляемых устройств CPE, которые используются в экземпляре SD-WAN (см. таблицы ниже).

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	40	2	3
до 100	6	8	40	2	3
до 250	8	16	40	2	3
до 500	8	16	40	2	6
до 1000	8	16	40	2	12
до 5000	8	16	40	2	60
до 10000	8	16	40	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

При необходимости подключения более 250 устройств CPE развертываются дополнительные кластеры контроллеров SD-WAN.

На этапе планирования ресурсов для развертывания экземпляра SD-WAN мы рекомендуем учитывать возможность использования переподписки. Максимальный коэффициент переподписки, доступный при использовании контейнеров, составляет 3. Коэффициент определяется следующими характеристиками экземпляра SD-WAN:

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

Программные требования

Для развертывания решения 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 веб-браузеры

Для работы с веб-интерфейсом оркестратора вы можете использовать следующие веб-браузеры:

- 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 могут быть использованы 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) для обеспечения отказоустойчивости. В нем 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 вам 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 появились следующие возможности и доработки:

- Проведен ребрендинг веб-интерфейса оркестратора в стиле "Лаборатории Касперского".
- Добавлена возможность переключения между светлой и темной темой веб-интерфейса оркестратора.
- Поддержка мультифакторной автоматической настройки (англ. Zero Touch Provisioning, ZTP) устройств CPE с использованием URL-активации.
- Поддержка протокола динамической маршрутизации BGP с быстрой сходимостью, которая обеспечивается протоколом BFD.
- Поддержка механизма BGP AS Prepend.
- Добавлена возможность распознавания и маршрутизации трафика приложений до уровня L7.
- Поддержка пассивного мониторинга качества каналов передачи данных.
- Добавлена возможность шифрования трафика, передающегося через туннели.

- Поддержка функции исправления ошибок Forward Error Correction (FEC) для устранения потерь пакетов трафика на нестабильных каналах передачи данных.
- Добавлена возможность дупликации пакетов трафика по альтернативным туннелям.
- Унифицирована прошивка устройств CPE и шлюзов SD-WAN.
- Добавлена возможность централизованного автоматического построения L2-туннелей Full-Mesh и Partial-Mesh между устройствами CPE.
- Добавлена возможность фильтрации маршрутной информации в протоколе динамической маршрутизации BGP с помощью списков управления доступом (англ. access lists, ACL).
- Добавлена возможность обработки фрагментированных пакетов трафика на устройствах CPE и шлюзах SD-WAN.
- Поддержка механизма фрагментации пакетов на интерфейсах SD-WAN.
- Поддержка сертифицированной операционной системы Astra Linux для развертывания центральных компонентов решения.
- Поддержка внеполосного (англ. out-of-band) управления устройствами CPE.
- Добавлена возможность централизованного обновления прошивок на устройствах CPE, а также назначения даты и времени установки новой прошивки.
- Добавлена возможность обновления центральных компонентов решения, обеспечивающих оркестрацию.
- Поддержка OpenStack (релиз Xena) в качестве VIM.
- Управление параметрами Trunk на OpenStack через графический конструктор.
- Добавлена возможность добавления поля `hostname` к пакету VNF.
- Пароль в параметрах LDAP теперь по умолчанию скрыт.
- Добавлена возможность ограничивать полосу пропускания трафика (проводить полисинг трафика) как для всех очередей при создании классов трафика, так и для каждой отдельной очереди на интерфейсах SD-WAN.
- Добавлена возможность перемаркировки поля `DSCP` исходящего трафика на уровне интерфейсов SD-WAN.
- Поддержка автоматической настройки соответствия стоимости (англ. cost) реальной пропускной способности (англ. bandwidth) канала передачи данных.
- Поддержка транспортного сервиса IP multicast.
- Максимальное количество динамических BGP-соседей увеличено до 512.

Архитектура решения

Kaspersky SD-WAN содержит следующие компоненты:

- **Оркестратор** – обеспечивает управление инфраструктурой решения, в том числе устройствами CPE, через графический веб-интерфейс. Обратите внимание, что оркестратор может управлять несколькими экземплярами SD-WAN.
- **Контроллер SD-WAN** – централизованно управляет по протоколу OpenFlow устройствами CPE, 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)** – менеджер, который обеспечивает конфигурацию **виртуальных сетевых функций** (англ. Virtual Network Functions, далее также VNF) и устройств CPE.

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

Все компоненты решения разворачиваются в центрах обработки данных (далее также ЦОДы), за исключением устройств CPE, которые устанавливаются на требуемых площадках.

Решение подразумевает развертывание отдельного экземпляра SD-WAN для каждого **тенанта**. Тенанты используются для обеспечения независимости сетей SD-WAN разных организаций друг от друга.

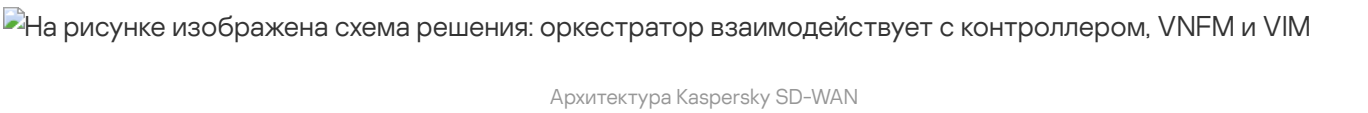
> Клиент вашей организации, которому выделяется логический набор сетевых и/или вычислительных ресурсов, для построения сети SD-WAN.

При создании и регистрации устройств CPE для отдельных клиентских тенантов, вы можете назначать эти устройства одному транспортному тенанту, если хотите построить сеть SD-WAN с использованием ограниченного количества устройств. В этом случае тенанты делят между собой контроллер SD-WAN, но имеют отдельные устройства, транспортные сервисы и веб-интерфейсы оркестратора.

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).



Архитектура Kaspersky SD-WAN

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 для обеспечения отказоустойчивости.

Контроллер SD-WAN в виде VNF или PNF

Вы можете развернуть контроллер SD-WAN в виде VNF или PNF. Для этого вам нужно использовать **пакет VNF** (англ. VNF package) или **пакет PNF** (англ. PNF package). Эти два пакета практически идентичны друг другу и содержат следующие данные:

Пакет в формате TAR или ZIP, который содержит данные, необходимые для развертывания и управления PNF.

Пакет в формате TAR или ZIP, который содержит данные, необходимые для развертывания и управления VNF.

- Папка /images – содержит образ виртуальной машины для контроллера SD-WAN. Файл образа имеет формат QCOW2. Эта папка не входит в состав пакета PNF.
- VNF-дескриптор или PNF-дескриптор – файл с именем vnfd или pnfd, который описывает параметры сетевой функции и имеет формат XML или YAML.
- Папка со скриптами – скрипты используются для конфигурации виртуальных машин.

Перед добавлением PNF в каталог веб-интерфейса оркестратора требуется развернуть контроллер (или кластер контроллеров) и два шлюза SD-WAN.

Резервирование и отказоустойчивость

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

- Отказ одного из центральных компонентов. Например, сеть SD-WAN сохраняет работоспособность при отказе **оркестратора**, **шлюза** или **контроллера SD-WAN**.

  Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

  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.

  Инструмент управления, мониторинга и диагностики сети SD-WAN, также отвечающий за виртуализацию сетевых функций (англ. Network Function Virtualization, NFV). Для управления оркестратором используется графический веб-интерфейс.

- Отказ или перегрузка каналов передачи данных между центральными компонентами при их георезервировании. *Георезервирование* – это размещение компонентов сети на географически разнесенных площадках для обеспечения надежности хранения данных.

- Отказ или перегрузка каналов передачи данных между **устройствами CPE** и шлюзами SD-WAN.

  Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Резервирование центральных компонентов решения

Kaspersky SD-WAN поддерживает несколько схем резервирования отдельных компонентов (см. таблицу ниже).

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.

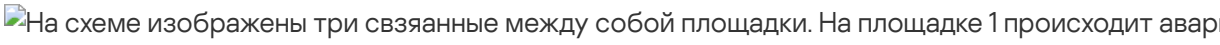
Для компонентов решения, которые резервируются по схеме N+1, развертываются два узла в разных ЦОД. Каждый из узлов находится в активном состоянии. Вы можете выбрать узел, к которому направляются запросы, с помощью виртуального IP-адреса или службы DNS.

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:

- Узел orc-dbs 2 и узел-арбитр orc-dbs 3 теряют связь с узлом orc-dbs 1, после чего выбирают новый основной узел.
- Узел-арбитр orc-dbs 3 не может быть основным узлом, поэтому им становится узел orc-dbs 2 и сообщает оркестратору о своей роли.
- Узел ctl 2 и узел-арбитр ctl 3 теряют связь с узлом ctl 1, после чего выбирают новый основной узел.
- Узел-арбитр ctl 3 не может быть основным узлом, поэтому им становится узел ctl 2 и сообщает оркестратору о своей роли.

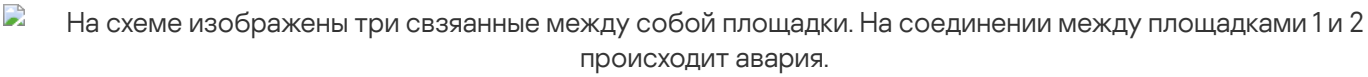
На рисунке ниже представлен пример аварии, в ходе которой выходят из строя узлы кластера компонентов решения на площадке 2.

Авария на площадке 2

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

- 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.
- 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.



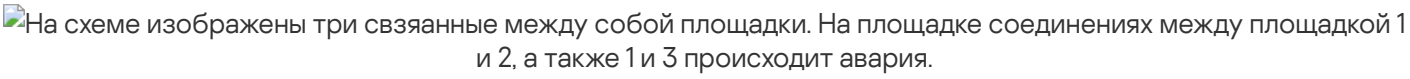
Авария на соединении между площадками 1 и 2

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

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

- 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:

- Узел orc-dbs 1 теряет связь с узлом orc-dbs 2.
- Узел orc-dbs 2 становится основным узлом и сообщает оркестратору о своей роли, потому что узел-арбитр orc-dbs 3 видит, что площадка 1 недоступна.
- Узел ctl 1 теряет связь с узлом ctl 2.
- 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 с помощью одновременного использования всех доступных каналов передачи данных, например интернет-каналов или LTE-каналов.

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* используется для равномерного распределения трафика по туннелям для предотвращения перегрузки отдельных туннелей и последующего возникновения 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.

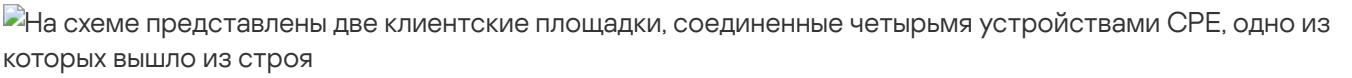
Режим Active/Standby

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.

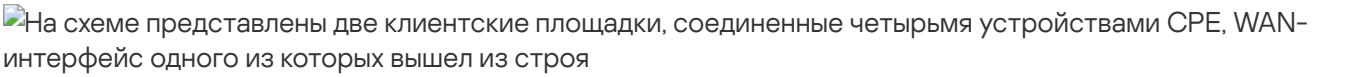
Вы можете настроить резервирование на уровне транспортных сервисов. В этом случае при создании транспортного сервиса указываются резервные сервисные интерфейсы (англ. reserve SI) на выбранном устройстве CPE или на другом устройстве. Мы рекомендуем создавать основной и резервный сервисные интерфейсы на 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:

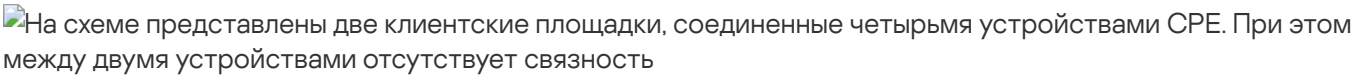
- Выход из строя одного из устройств CPE.

  
  На схеме представлены две клиентские площадки, соединенные четырьмя устройствами CPE, одно из которых вышло из строя

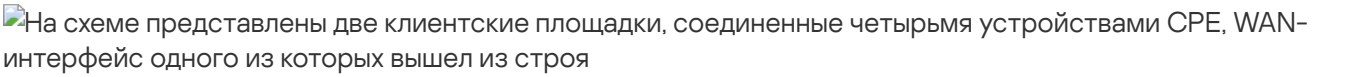
- Выход из строя WAN-интерфейса одного из устройств CPE.

  
  На схеме представлены две клиентские площадки, соединенные четырьмя устройствами CPE, WAN-интерфейс одного из которых вышел из строя

- Выход из строя связности между двумя устройствами CPE.

  
  На схеме представлены две клиентские площадки, соединенные четырьмя устройствами CPE. При этом между двумя устройствами отсутствует связность

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

  
  На схеме представлены две клиентские площадки, соединенные четырьмя устройствами CPE, WAN-интерфейс одного из которых вышел из строя

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 их сообщением. В каждой плоскости происходят следующие процессы:

Осуществляет передачу пакетов трафика. Плоскость передачи данных образуют устройства CPE.

Контролирует передачу пакетов трафика по сети через устройства CPE. В плоскость управления трафиком входят оркестратор и контроллер SD-WAN.

- аутентификация и авторизация пользователей;

- использование безопасных протоколов управления;
- шифрование управляющего трафика.

Для безопасности **тенантов** применяется шифрование данных и изоляция трафика в рамках каждого отдельного тенанта и сетевого сервиса. Решение также поддерживает безопасное подключение **устройств CPE**.

Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Клиент вашей организации, которому выделяется логический набор сетевых и/или вычислительных ресурсов, для построения сети SD-WAN.

Аутентификация и авторизация пользователей

Управление Kaspersky SD-WAN осуществляется через веб-интерфейс оркестратора или API. Устройства CPE также могут иметь графические интерфейсы. Остальные компоненты решения не имеют графического интерфейса. Пользователю нужно авторизоваться, чтобы получить доступ к управлению решением.

Вы можете хранить информацию об учетных записях пользователей в локальной базе данных или импортировать ее из внешней системы LDAP. Для интеграции с внешними службами каталогов решение поддерживает протоколы LDAP и LDAPS.

При добавлении сервера LDAP вам нужно указать путь к месту хранения учетных записей пользователей, а также учетную запись с правами read-only, которую оркестратор будет использовать для поиска учетных записей. Решение назначает роль каждой учетной записи или группе Microsoft Active Directory, которую вы добавляете с помощью сервера LDAP и при необходимости привязывает их к тенанту.

Использование безопасных протоколов управления

Мы рекомендуем использовать протокол HTTPS при взаимодействии с сетью SD-WAN через веб-интерфейс оркестратора или API.

Вы можете загрузить в веб-интерфейс оркестратора 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 и контроль конфигурации

Решение использует следующие механизмы для идентификации устройств 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 требуемой площадке.
- Двухфакторная аутентификация – клиент получает ключ, который требуется ввести на устройстве CPE для его активации.

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.

Вы можете разрешить или запретить локальное изменение загруженной конфигурации устройства CPE.

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:

> 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.

> 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. Для настройки отдельных компонентов решения вы можете использовать разделы, которые отображаются в навигационной панели в левой части страницы (см. рисунок ниже). Когда вы переходите в один из разделов, его содержимое отображается справа.


На скриншоте представлена навигационная панель решения

Навигационная панель

Навигационная панель содержит следующие разделы:

- **Обозреватель** (раздел Обозреватель) – в этом разделе вы можете просматривать информацию о текущем состоянии компонентов решения, таких как **устройства CPE**, **VNF** и **PNF**.

  Заранее развернутая сетевая функция, которая в готовом виде загружается в веб-интерфейс оркестратора. Оркестратор может осуществлять дальнейшую конфигурацию PNF.

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

  Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

- **Инфраструктура** (раздел Инфраструктура) – в этом разделе вы можете настраивать вашу сетевую инфраструктуру, например создавать домены, а также добавлять ЦОДы и **VIM**. Кроме того, здесь отображаются все доступные вам **контроллеры SD-WAN**, и вы можете перейти в отдельное меню настройки каждого из них.

  Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

  Менеджер, обеспечивающий управление и мониторинг вычислительных и сетевых ресурсов, а также ресурсов хранения в виртуальной инфраструктуре. С его помощью VNF взаимодействуют со всеми этими ресурсами.

- **Каталог** () – в этом разделе вы можете выполнять следующие действия в зависимости от вашей роли:

  - как администратор решения вы можете загружать VNF/PNF и использовать их при создании шаблонов сетевых сервисов;
  - как администратор тенанта вы можете создавать сетевые сервисы, используя графический конструктор.

- **SD-WAN** (раздел SD-WAn) – в этом разделе вы можете настраивать устройства CPE, экземпляры SD-WAN и UNI, а также управлять прошивками и сертификатами устройств.

- **Планировщик** (Иконке в форме часов) – в этом разделе вы можете настраивать отложенный запуск задач и назначать их на определенное время.

- **Журнал** (раздел Журнал) – в этом разделе вы можете просматривать журналы работы различных компонентов решения. Например, здесь отображаются внесенные другими пользователями изменения в параметры устройств CPE.

- **Тенанты** (тенанты) – в этом разделе вы можете настраивать тенантов и предоставлять им в пользование различные компоненты решения, например устройства CPE, VIM и UNI. Здесь вы также можете подключиться к веб-интерфейсу оркестратора тенанта в качестве администратора.

- **Пользователи** (Иконка в виде фигурок двух пользователей) – в этом разделе вы можете настраивать учетные записи пользователей и определять для них роли, а также назначать пользователей тенантам. Здесь вы также можете настраивать права доступа пользователей, и доменную аутентификацию.

- **Подтверждение** (раздел Подтверждение) – в этом разделе вы можете управлять запросами на подтверждение. Пользователи, учетная запись которых имеет статус *read-only*, отправляют запросы на подтверждение, чтобы выполнять действия с компонентами решения.

Когда вы переходите в один из разделов, навигационная панель отображается в свернутом виде. Вам нужно навести курсор мыши на значок одного из разделов, чтобы развернуть навигационную панель. Для выключения функции автоматического сворачивания навигационной панели вы можете нажать на кнопку разворачивания расширение панели навигации.

Лицензирование Kaspersky SD-WAN

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky SD-WAN.

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".

Параметры компонентов Kaspersky SD-WAN в веб-интерфейсе

В этом разделе содержится информация о том, как перейти в разделы и подразделы веб-интерфейса оркестратора, которые вы можете использовать для настройки требуемых компонентов решения. Сам процесс настройки компонентов описывается в соответствующих разделах справки.

Управление инфраструктурой

Чтобы перейти в раздел управления инфраструктурой решения,

в навигационной панели перейдите в раздел **Инфраструктура**.

Откроется страница со списком компонентов, с помощью которых развернут ваш экземпляр SD-WAN. По умолчанию выбрана вкладка **Сетевые ресурсы**, на которой отображаются все доступные контроллеры SD-WAN и их узлы.

Параметры подключения к Zabbix

Чтобы перейти в раздел настройки подключения к Zabbix,

в навигационной панели перейдите в раздел **Мониторинг**.

Откроется страница с параметрами подключения вашего экземпляра SD-WAN к Zabbix-серверу.

Параметры сетевых сервисов

Чтобы перейти в раздел настройки сетевых сервисов,

в навигационной панели перейдите в раздел **Каталог**.

Откроется страница настройки сетевых сервисов с графическим конструктором. Если у вас уже есть развернутый сетевой сервис, он отобразится справа.

Параметры устройства CPE

Чтобы открыть область настройки устройства CPE:

1. В навигационной панели перейдите в раздел **SD-WAN**.
2. Нажмите на устройство CPE, которое требуется настроить.

В нижней части страницы откроется область настройки с выбранной по умолчанию вкладкой **Конфигурация**. Вы можете нажать на кнопку развертывания , чтобы развернуть область настройки на всю страницу.

Параметры шаблона CPE

Чтобы открыть область настройки шаблона CPE:

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

2. Нажмите на шаблон CPE, который требуется настроить.

В нижней части страницы откроется область настройки с выбранной по умолчанию вкладкой **Информация**. Вы можете нажать на кнопку развертывания , чтобы развернуть область настройки на всю страницу.

Параметры экземпляра SD-WAN

Чтобы открыть область настройки экземпляра SD-WAN:

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

2. Нажмите на экземпляр SD-WAN, который требуется настроить.

В нижней части страницы откроется область настройки с выбранной по умолчанию вкладкой **Информация**. Вы можете нажать на кнопку развертывания , чтобы развернуть область настройки на всю страницу.

Параметры шаблона экземпляра SD-WAN

Чтобы открыть область настройки шаблона экземпляра SD-WAN:

1. В навигационной панели перейдите в раздел **SD-WAN → Шаблоны экземпляров SD-WAN**.

2. Нажмите на шаблон экземпляра SD-WAN, который требуется настроить.

В нижней части страницы откроется область настройки с выбранной по умолчанию вкладкой **Информация**. Вы можете нажать на кнопку развертывания , чтобы развернуть область настройки на всю страницу.

Управление тенантами

Чтобы перейти в раздел управления тенантами,

в навигационной панели перейдите в раздел **Тенанты**.

Откроется страница со списком созданных тенантов и доступных для них компонентов.

Параметры пользователей

Чтобы перейти в раздел настройки пользователей,

в навигационной панели перейдите в раздел **Пользователи**.

Откроется страница со списком пользователей.

Дополнительное меню настройки веб-интерфейса

В дополнительном меню настройки веб-интерфейса вы можете управлять передачей трафика в рамках развернутого экземпляра SD-WAN, например создавать транспортные сервисы и указывать параметры качества обслуживания. Переход в это меню осуществляется через развернутый контроллер SD-WAN.

Чтобы перейти в дополнительное меню настройки веб-интерфейса:

1. В навигационной панели перейдите в раздел **Инфраструктура**.
2. Нажмите на кнопку **Управление** рядом с требуемым контроллером SD-WAN и в раскрывающемся списке выберите **Настроить**.

Откроется дополнительное меню настройки веб-интерфейса оркестратора, и по умолчанию вы перейдете в раздел **Узлы контроллера**.

Свойства контроллера SD-WAN

Чтобы перейти к списку свойств контроллера SD-WAN:

1. В навигационной панели перейдите в раздел **Инфраструктура**.
2. Нажмите на кнопку **Управление** рядом с требуемым контроллером SD-WAN и в раскрывающемся списке выберите **Параметры**.

   Отобразится список свойств контроллера SD-WAN, как изменяемых (Reload и Runtime), так и неизменяемых (Read-only).
3. При необходимости отобразить только изменяемые свойства выберите вкладку **Изменяемые параметры**.

Над списком свойств находится поле поиска , с его помощью вы можете найти свойства по методу изменения, имени, а также текущему или планируемому значению.

Базовая настройка решения

После развертывания решения вам нужно выполнить его базовую настройку, прежде чем вы сможете перейти к выполнению обычных задач.

Авторизация в веб-интерфейсе оркестратора

Чтобы авторизоваться в веб-интерфейсе оркестратора:

1. В адресной строке браузера введите IP-адрес или имя сервера Kaspersky SD-WAN.
2. На открывшейся странице авторизации 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 авторизации откроется раздел **Обозреватель**.

Установка и сброс страницы по умолчанию

Страница по умолчанию – это раздел или подраздел веб-интерфейса оркестратора (включая дополнительное меню), который автоматически отображается после вашей авторизации.

Чтобы установить или сбросить страницу по умолчанию:

1. Перейдите в раздел/подраздел веб-интерфейса оркестратора, который вы хотите установить как страницу по умолчанию.
2. В навигационной панели снизу нажмите на кнопку настройки и в раскрывающемся списке выберите **Установить как страницу по умолчанию**.

   Вверху отобразится сообщение `Установлена страница по умолчанию`.
3. При необходимости сбросить страницу по умолчанию снова нажмите на кнопку настройки и в раскрывающемся списке выберите **Сбросить страницу по умолчанию**.

   Вверху отобразится сообщение `Параметры страницы по умолчанию были сброшены`. Теперь страницей по умолчанию является раздел **Обозреватель**.

Переключение между светлой и темной темой

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

в навигационной панели снизу нажмите на кнопку настройки и в раскрывающемся списке выберите одно из следующих значений:

- **Включить темную тему**.
- **Включить светлую тему**.

Ограничение продолжительности пользовательской сессии при бездействии

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

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

1. В навигационной панели снизу нажмите на кнопку настройки и в раскрывающемся списке выберите **Установить время истечения сессии**.

2. В открывшемся окне укажите время в секундах, по истечении которого требуется прекратить вашу сессию при бездействии. Диапазон значений: от 60 до 86400. По умолчанию указано значение `3600`.

3. Нажмите на кнопку **OK**.

Просмотр активных пользовательских сессий

Вы можете просматривать список пользователей авторизованных в веб-интерфейсе оркестратора с использованием вашей учетной записи.

Чтобы просмотреть активные пользовательские сессии:

1. В навигационной панели снизу нажмите на кнопку настройки и в раскрывающемся списке выберите **Сессии**.

   Отобразится таблица с активными пользовательскими сессиями.

2. При необходимости прекратить пользовательскую сессию нажмите на кнопку **Аннулировать** рядом с ней.

   Пользовательская сессия будет прекращена.

Настройка уровня детализации журналов Docker-контейнеров

Kaspersky SD-WAN автоматически ведет журналы Docker-контейнеров, используемых для развертывания компонентов решения и поддержания их работы. Вы можете выбрать уровень детализации этих журналов, чтобы настроить количество включаемой в них информации для более удобного восстановления работы контейнеров, а также их мониторинга.

Поддерживаются следующие уровни детализации:

- **ТРАССИРОВКА** – включать в журналы наиболее полную информацию, например отладочные операторы (англ. debug statements), для расширенного поиска и устранения проблем.

- **ОТЛАДКА** – включать в журналы детализированную информацию, например 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 потенциально могут скомпрометировать работу контейнера.

- **ОШИБКА** – включать в журналы записи об ошибках или исключениях которые потенциально могут скомпрометировать работу контейнера. Такие записи зачастую требуют незамедлительного вмешательства со стороны пользователя.

Чтобы настроить уровень детализации журналов Docker-контейнеров:

1. В навигационной панели снизу нажмите на кнопку настройки и в раскрывающемся списке выберите **Общие параметры журналирования**.

2. Выполните одно из следующих действий:

   - Выберите уровень детализации журналов для всех модулей Docker-контейнеров в верхней части страницы.

   - Выберите уровень детализации журналов для каждого отдельного модуля Docker-контейнеров.

Переход к API оркестратора

Чтобы перейти к API оркестратора,

в навигационной панели снизу нажмите на кнопку перехода к API question_mark_icon.

Отобразится список API-команд, доступных для управления оркестратором.

Изменение пароля учетной записи администратора

Чтобы изменить пароль учетной записи администратора:

1. В навигационной панели перейдите в раздел **Пользователи**.

2. В списке пользователей нажмите на учетную запись администратора.

3. Нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Изменить пароль**.

4. В открывшемся окне укажите новый пароль в двух полях:

   - **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 .

   - **Подтверждение пароля**.

5. Нажмите на кнопку **Сохранить**.

Пароль учетной записи администратора будет изменен. Вам потребуется использовать этот пароль во время следующей авторизации в веб-интерфейсе оркестратора.

Создание домена

Домен – это логическая группа сетевых ресурсов, которые могут располагаться в одном или нескольких центрах обработки данных. Вы можете разделять сетевые ресурсы, обеспечивающие функционирование решения, между разными доменами, после чего индивидуально настраивать каждый домен.

Чтобы создать домен:

1. На странице управления инфраструктурой решения нажмите на кнопку **+ Домен**.
2. В открывшемся окне настройте параметры домена, выполнив следующие действия:
   - В поле **Имя** введите имя домена. Диапазон значений: от 1 до 50 символов.
   - В поле **Описание** введите краткое описание домена. Максимальная длина: 100 символов.
3. Нажмите на кнопку **Сохранить**.

Домен отобразится в панели **Ресурсы**. Теперь этот домен можно выбрать при добавлении центров обработки данных, чтобы объединить их в одну логическую группу.

Вы можете выполнить одно из следующих действий с доменом, нажав на кнопку настройки рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры домена, выбрав **Изменение домена**.
- Удалить домен, выбрав **Удаление домена**.

Добавление центра обработки данных

Центральные компоненты Kaspersky SD-WAN, за исключением **устройств CPE**, размещаются в центрах обработки данных. Обратите внимание, что при добавлении ЦОД в веб-интерфейс оркестратора вам нужно указать URL-адрес развернутого **VNFM**.

> Инструмент конфигурации VNF, развернутых оркестратором.

> Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Чтобы добавить центр обработки данных:

1. На странице управления инфраструктурой решения нажмите на кнопку **+ ЦОД**.

2. В открывшемся окне настройте параметры ЦОД, выполнив следующие действия:

   - В поле **Имя** введите имя ЦОД. Диапазон значений: от 1 до 20 символов.
   - В поле **Описание** введите краткое описание ЦОД. Максимальная длина: 100 символов.
   - В раскрывающемся списке **Домен** выберите домен, в который требуется добавить ЦОД.
   - В поле **VNFM URL** введите URL-адрес менеджера виртуальных функций, развернутого в ЦОД. Вы можете убедиться в доступности VNFM, нажав на кнопку **Проверить соединение**.
   - В поле **Адрес** введите почтовый адрес ЦОД.

3. Нажмите на кнопку **Сохранить**.

ЦОД отобразится в панели **Ресурсы**. Вы можете выполнить одно из следующих действий с ЦОД, нажав на кнопку настройки рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры ЦОД, выбрав **Изменение ЦОДа**.
- Мигрировать ЦОД, выбрав **Мигрировать**. Вы можете мигрировать центры обработки данных для выполнения следующих задач:
  - Объединение распределенных площадок – миграция ЦОД позволяет объединить несколько распределенных площадок в одной локации для снижения стоимости аренды, количества выполняемых операций, а также улучшения общей производительности за счет централизации процессов управления и назначения ресурсов.
  - Улучшение производительности сети – миграция ЦОД позволяет переместить его ближе к офисам вашей организации или пользователем для снижения времени задержки при передаче данных.
  - Повышение масштабируемости – миграция ЦОД упрощает процесс развертывания нового оборудования и/или облачных сервисов в соответствии с требованиями вашей организации.
  - Повышение отказоустойчивости – миграция ЦОД в географически удаленную локацию повышает работоспособность вашей сети в случае возникновения неисправностей, особенно в сочетании со способностью сети SD-WAN динамически маршрутизировать трафик и одновременно использовать несколько каналов передачи данных.
  - Экономия средств – миграция ЦОД позволяет переместить его в более экономически выгодную локацию, в которой, например возможно использование облачных сервисов или совместная аренда оборудования с другими организациями.
- Удалить ЦОД, выбрав **Удаление ЦОДа**.

Добавление VIM

Перед развертыванием **VNF** в центре обработки данных вам нужно добавить для него как минимум один **VIM**. В Kaspersky SD-WAN используется VIM от OpenStack.

> Менеджер, обеспечивающий управление и мониторинг вычислительных и сетевых ресурсов, а также ресурсов хранения в виртуальной инфраструктуре. С его помощью VNF взаимодействуют со всеми этими ресурсами.

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

Чтобы добавить VIM:

1. На странице управления инфраструктурой решения нажмите на кнопку **+ VIM**.

2. В открывшемся окне настройте параметры VIM, выполнив следующие действия:

   - В раскрывающихся списках **Домен** и **ЦОД** выберите домен и ЦОД, для которого требуется добавить VIM.
   - В поле **Имя** введите имя VIM.
   - В поле **IP** введите IP-адрес или доменное имя для подключения оркестратора к VIM.
   - В поле **Порт** введите номер порта для подключения оркестратора к VIM. По умолчанию указано значение `5000`.
   - В раскрывающемся списке **Протокол** выберите протокол для подключения оркестратора к VIM:
     - **http** – это значение выбрано по умолчанию.
     - **https**.
   - В поле **Имя пользователя** введите имя пользователя учетной записи OpenStack с правами администратора для авторизации в VIM.
   - В поле **Пароль** введите пароль учетной записи OpenStack с правами администратора для авторизации в VIM.
   - В поле **Проект администратора** введите имя проекта администратора OpenStack для авторизации в VIM.
   - В поле **Домен** введите имя OpenStack-домена.
   - В раскрывающемся списке **За NAT** выберите, находится ли VIM за NAT (Network Address Translation):
     - **Включено** – VIM находится за NAT.
     - **Выключено** – VIM не находится за NAT. Это значение выбрано по умолчанию.
   - В поле **Переподписка ЦП** введите коэффициент переподписки при предоставлении виртуальных процессорных ядер. По умолчанию указано значение `1`.
   - В поле **Переподписка ОЗУ** введите коэффициент переподписки оперативной памяти. По умолчанию указано значение `1`.
   - В поле **Переподписка диска** введите коэффициент переподписки дискового пространства. По умолчанию указано значение `1`.
   - В поле **Количество потоков** введите максимальное количество потоков при взаимодействии оркестратора с VIM. По умолчанию указано значение `1`.

- В раскрывающемся списке **Кластер SDN** выберите SDN-кластер, к которому подключен OpenStack, или значение **None**, если OpenStack не подключен к SDN-кластеру.

- В поле **Диапазон VLAN ID** введите максимальное количество VLAN для OpenStack. Диапазон значений: от 0 до 4094.

- В поле **Имя physnet для SR-IOV** введите имя physnet для сетей с типом подключения SR-IOV. Этот тип подключения используется с сегментацией VLAN.

- В поле **Физическая VLAN-сеть** введите имя physnet для VLAN-сетей.

3. Если в раскрывающемся списке **Кластер SDN** вы выбрали SDN-кластер, укажите параметры подключения к кластеру, выполнив следующие действия:

   - В поле **OpenStack-сеть** введите имя сети OpenStack, к которой подключен VIM.

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

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

   - В раскрывающемся списке **Вычислительная группа** выберите группу интерфейсов, через которую вычислительные узлы OpenStack подключены к SDN-кластеру.

4. Если в раскрывающемся списке **Кластер SDN** вы выбрали **None**, выполните следующие действия:

   - В поле **Имя physnet для FLAT** введите имя physnet для плоских сетей (англ. flat networks).

   - В поле **Имя physnet для VXLAN** введите имя physnet для VXLAN-сетей.

   - В раскрывающемся списке **Сегментация управляющей сети** выберите тип сегментации используемый управляющей сетью:

     - **VLAN**.

     - **VXLAN**.

   - В поле **ID управляющего сегмента** введите ID сегмента управляющей сети. Диапазон значений: от 0 до 16 000 000.

   - В раскрывающемся списке **Port security** выберите, включена функция Port sercurity или нет:

     - **Включено**.

     - **Выключено**.

     Функция Port security используется для повышения уровня безопасности сети на уровне Ethernet-портов коммутатора. Она предотвращает не авторизованный доступ к сети за счет ограничения количества 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.

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

5. Нажмите на кнопку **Сохранить**.

VIM отобразится на вкладке **Вычислительные ресурсы**. Вы можете выполнить одно из следующих действий с VIM, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры VIM, выбрав **Изменить**.
- Показать использование VIM, выбрав **Использование**.
- Удалить VIM, выбрав **Удалить**.

Создание диапазона IP-адресов (IPAM)

Диапазоны IP-адресов позволяют разделять управляющий и пользовательский трафик для внутреннего управления (англ. in-band management) сетью SD-WAN, повышения ее производительности а также обеспечения безопасности, мониторинга, настройки и технической поддержки сетевых устройств. Например, если управляющий трафик отделен от пользовательского, администраторы могут удаленно подключаться к сетевым устройствам для установки обновлений, исправления проблем и внесения изменений в конфигурацию. Наличие отдельного диапазона IP-адресов также позволяет использовать более детализированные политики безопасности, такие как списки управления доступом и правила брандмауэра, для защиты управляющего трафика и критически важных компонентов сети SD-WAN.

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

Чтобы создать диапазон IP-адресов:

1. На странице управления инфраструктурой решения нажмите на кнопку **+ Подсеть**.
2. В открывшемся окне настройте параметры подсети, выполнив следующие действия:
   - В раскрывающихся списках **Домен** и **ЦОД** выберите домен и ЦОД, для которого требуется создать диапазон IP-адресов.
   - В поле **Имя** введите имя диапазона IP-адресов.
   - В раскрывающемся списке **Версия IP** выберите версию IP-адресов в диапазоне:
     - **IPv4** – это значение выбрано по умолчанию.
     - **IPv6**.
   - В поле **CIDR** введите IP-адрес сети, для которой вы создаете диапазон IP-адресов, а также маску подсети. Использование CIDR-нотации позволяет указать размер сети, в рамках которой осуществляется назначение IP-адресов из диапазона. Формат значения: <IP-адрес>/<маска подсети>, например 192.168.2.0/24.
   - В поле **Шлюз** введите IP-адрес шлюза по умолчанию для сетевых устройств, которым назначаются IP-адреса из диапазона. Шлюз по умолчанию в сети SD-WAN обеспечивает коммуникацию между устройствами из локальной и внешних сетей.
   - В блоке **Диапазон IP** создайте диапазон IP-адресов, нажав на кнопку **+ Добавить** и указав требуемые значения в отобразившихся полях. Вы можете создать несколько диапазонов.

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

- В блоке **Статические маршруты** создайте статический маршрут, нажав на кнопку + **Добавить** и указав статический маршрут в отобразившемся поле. Компоненты решения получают статический маршрут вместе с IP-адресами из диапазона. Вы можете создать несколько маршрутов. Наличие статических маршрутов позволяет управлять маршрутизацией трафика между сегментами сети или подсетями для выполнения требуемых задач, таких как оптимизация процесса передачи трафика, обеспечение маршрутизации определенного вида трафика по указанному назначению, а также установка соединения между двумя удаленным площадками.

3. Нажмите на кнопку **Сохранить**.

Диапазон IP-адресов отобразится на вкладке **IPAM**. Вы можете выполнить одно из следующих действий с диапазоном IP-адресов, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры диапазона IP-адресов, выбрав **Изменить**.

- Удалить диапазон IP-адресов, выбрав **Удалить**.

Создание тенанта

Тенанты используются для логического разделения и изоляции разных субъектов и групп внутри сети SD-WAN. Таким образом достигается *мультитенантность*, в рамках которой несколько независимых организаций, подразделений или клиентов могут использовать одну и ту же физическую инфраструктуру и при этом иметь собственные виртуальные сети. Мультитенантная сеть SD-WAN имеет следующие преимущества:

- Изолированность – тенанты обеспечивают полную изоляцию сетевых ресурсов и трафика одного субъекта или группы от других, предотвращая не авторизованный доступ и тем самым повышая защищенность и конфиденциальность виртуальных сетей.

- Управляемость – тенанты могут определять политики управления и конфигурации в соответствии с существующими требованиями и имеют более полный контроль над собственными сетями и приложениями.

- Масштабируемость – тенанты увеличивают горизонтальную масштабируемость сети, позволяя создавать большое количество независимых субъектов с доступом к общей физической инфраструктуре, что в свою очередь обеспечивает более эффективное использование ресурсов.

- Гибкость – использование тенантов позволяет адаптировать сеть к новым требованиям организаций, подразделений и клиентов, например посредством создания новых сетевых сервисов или QoS-политик.

Вы можете назначать тенантам следующие компоненты Kaspersky SD-WAN:

- VIM.

- UNI.

- Компоненты для создания сетевых сервисов, такие как VNF, PNF и шаблоны.

- Пользователей и группы пользователей.
- Устройства CPE.

Чтобы создать тенанта:

1. В разделе управления тенантами в блоке **Тенанты** выполните одно из следующих действий:
   - Если вы создаете первого тенанта, в поле **Имя** введите имя тенанта и нажмите на кнопку создания  кнопка в виде знака плюс.
   - Если вы создаете последующих тенантов, нажмите на кнопку **+ Тенант**, затем в поле **Имя** введите имя тенанта и нажмите на кнопку создания  кнопка в виде знака плюс.
2. Назначьте тенанту VIM, выполнив следующие действия в блоке **VIM**:
   a. Нажмите на кнопку **+ Изменить**.
   b. В открывшемся окне выберите требуемый VIM, указав домен и ЦОД, к которому он относится.
   c. Нажмите на кнопку **Сохранить**.
3. Назначьте тенанту группу пользователей, выполнив следующие действия в блоке **Группы**:
   a. Нажмите на кнопку **+ Изменить**.
   b. В открывшемся окне выберите требуемые группы пользователей.
   c. Нажмите на кнопку **Сохранить**.
4. Назначьте тенанту сетевые компоненты, установив флажки рядом с ними в блоке **Каталог**:

   > Если вы назначаете тенанту шаблон сетевого сервиса, ему становятся доступны все содержащиеся в этом шаблоне сетевые функции.

5. Убедитесь, что для тенанта развернуты все требуемые контроллеры и шлюзы SD-WAN с помощью блока **Сервисы SD-WAN**.
6. Определите объем доступных для тенанта вычислительных ресурсов, выполнив следующие действия в блоке **Ресурсы**:
   a. Перейдите к настройке вычислительных ресурсов, нажав на кнопку настройки в верхней части блока.
   b. Нажмите на кнопку изменения объема ∞ рядом с одним из следующих вычислительных ресурсов, после чего введите требуемый объем:
      - **ЦП** – виртуальные процессорные ядра.
      - **ОЗУ** – оперативная память.
      - **Диск** – дисковое пространство.
   c. Нажмите на кнопку сохранения  checkbox_icon.
7. Просмотрите список созданных в рамках тенанта запросов на обслуживание в блоке **Запросы**.

8. Назначьте тенанту пользователей, выполнив следующие действия в блоке **Пользователи**:

   a. Нажмите на кнопку **+ Изменить**.

   b. В открывшемся окне выберите требуемых пользователей.

   c. Нажмите на кнопку **Сохранить**.

9. Создайте для тенанта устройство CPE, нажав на кнопку **+ Устройство CPE** в блоке **Устройства CPE**.

10. При необходимости авторизуйтесь в веб-интерфейсе оркестратора как администратор тенанта, нажав на кнопку **Подключиться как тенант**.

Вы можете выполнить одно из следующих действий с тенантом, нажав на кнопку настройки рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры тенанта, выбрав **Изменить**.
- Удалить тенанта, выбрав **Удалить**.

Просмотр журналов

Журналы используются для диагностирования ошибок, возникающих при работе решения, а также для осуществления технической поддержки. Kaspersky SD-WAN ведет журналы, в которых отображаются следующие типы записей:

- Задачи, выполняемые пользователем. Например, запись о добавлении **VIM** пользователем с ролью администратора.

  > Менеджер, обеспечивающий управление и мониторинг вычислительных и сетевых ресурсов, а также ресурсов хранения в виртуальной инфраструктуре. С его помощью VNF взаимодействуют со всеми этими ресурсами.

- События, происходящие во время работы решения. Например, подключение туннеля. Если произошедшее событие связано с выполнением определенной задачи, эта связь будет отображена в соответствующей записи журнала.
- Запросы на обслуживание к определенным компонентам решения. Например, запрос на регистрацию **устройства CPE**.

  > Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Для каждой записи в журнале отображается статус, точное время выполнения, а также связанный с ней пользователь. По умолчанию журнал отображает записи за последние 24 часа, но вы можете указать другой временной интервал.

> 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 навигационной панели перейдите в раздел **Журналы**.
2. В панели **Ресурсы** выберите компонент решения, для которого требуется отобразить записи журнала.
3. Для просмотра записей определенного типа выберите соответствующую вкладку над списком записей журнала:
   - **Задачи**.
   - **События**.
   - **Сервисные запросы** – вы можете открыть пошаговый журнал выполнения запроса на обслуживание с подробной информацией о каждом шаге, нажав на идентификатор ID. Журнал содержит информацию о шагах, на которых произошли ошибки, а также подробное описание самих ошибок.
4. По умолчанию в журнале отображаются задачи, события и запросы на обслуживание за весь период и с любыми статусами. Вы можете отобразить только нужные вам записи с помощью фильтра в верхней части страницы:
   - По статусу – например, в списке задач можно отфильтровать задачи в статусе *Ожидают* или *Выполняются*, а в списке событий отфильтровать потенциально опасные события (*Предупреждения*).
   - По времени – например, можно отобразить записи за год, за месяц или за произвольно заданный временной интервал.

Просмотр запросов на обслуживание

Запросы на обслуживание – это задачи, которые выполняются во время работы одного из компонентов решения. Вы можете просматривать запросы на обслуживание в веб-интерфейсе оркестратора следующим образом:

- В разделе **Тенанты** – запросы на обслуживание отдельного тенанта.
- В подразделе **Устройства CPE** – запросы на обслуживание отдельного устройства.
- В подразделе **Экземпляры SD-WAN** – запросы на обслуживание всего экземпляра SD-WAN.

Для каждого такого запроса отображается статус, а также время, в течение которого он выполнялся.

Чтобы просмотреть запросы на обслуживание:

1. Перейдите к просмотру запросов на обслуживание одним из следующих способов:
   - В разделе управления тенантами в блоке **Тенанты** выберите требуемого тенанта.

     Запросы на обслуживание отобразятся в блоке **Запросы**.
   - В области настройки устройства CPE или экземпляра SD-WAN выберите вкладку **Запросы на обслуживание**.

     Запросы на обслуживание отобразятся в таблице.
2. При необходимости выполните следующие действия:

- Откройте пошаговый журнал выполнения запроса на обслуживания с подробной информацией о каждом шаге, нажав на его идентификатор ID. Журнал содержит информацию о шагах, на которых произошли ошибки, а также подробное описание самих ошибок.
- Удалите запрос на обслуживание, нажав на кнопку **Удалить** рядом с ним.
- Если вы просматриваете запросы на обслуживание в подразделе **Устройства CPE** или **Экземпляры SD-WAN**, нажмите на одну из следующих кнопок в блоке **Действия**:
  - **Обновить запросы на обслуживание** – обновить таблицу с запросами на обслуживание.
  - **Удалить все запросы на обслуживание** – удалить все запросы на обслуживание из таблицы.
  - **Отменить все запросы на обслуживание** – прекратить выполнение всех запросов на обслуживание. Кнопка отображается только при просмотре запросов на обслуживание в подразделе **Устройства CPE**.

Работа с пользователями

Пользователям необходимо авторизоваться в веб-интерфейсе оркестратора для работы с Kaspersky SD-WAN. Вы можете создавать 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 требуемому серверу.

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

При создании как отдельных пользователей, так и групп, им можно назначать права доступа, определяющие, какие разделы и/или подразделы веб-интерфейса они могут использовать.

Настройка подключения оркестратора к удаленному LDAP-серверу

Вам нужно настроить подключение оркестратора к удаленному LDAP-серверу, чтобы ваши пользователи могли авторизоваться в веб-интерфейсе, используя хранящиеся на этом сервере учетные данные. 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. На странице настройки пользователей выберите вкладку **Источники аутентификации**.
2. Нажмите на кнопку **+ LDAP**.

3. В отобразившейся области настройки настройте параметры подключения, выполнив следующие действия:

   - В поле **Имя** введите имя LDAP-подключения для отображения в оркестраторе.
   - В поле **Домен** введите FQDN домена, в котором находится LDAP-сервер. Оркестратор использует FQDN для подключения к LDAP-серверу и его аутентификации.
   - В поле **Domain Alias** введите альтернативное имя домена (как правило, NETBIOS-имя). Псевдоним используется при создании и авторизации пользователей наряду с FQDN домена, например, если FQDN домена – example.com, а псевдоним – example, вы можете вводить следующие значения:
     - `admin@example.com`;
     - `admin@example`;
     - `example.com\admin`;
     - `example\admin`.
   - В поле **LDAP-хост** введите имя LDAP-сервера. Поддерживаются два формата значения:
     - Стандартный LDAP-сервер – ldap://ldap.example.com:<`номер порта`>. Порт по умолчанию: 389.
     - LDAP-сервер с SSL-аутентификацией – ldaps://ldap.example.com:<`номер порта`>. Порт по умолчанию: 636.
   - В поле **Base DN** введите путь, который оркестратор должен использовать для поиска учетных записей пользователей на LDAP-сервере. Поддерживаются два формата значения:
     - OpenLDAP – ou=Users,ou=system.
     - Microsoft Active Directory – DC=company,DC=com.
   - В раскрывающемся списке **Поиск атрибута** выберите LDAP-атрибут, который оркестратор должен использовать для поиска учетных записей пользователей:
     - **uid (for OpenLDAP)** – для поиска пользователей в OpenLDAP. Атрибутом может быть уникальное имя или идентификатор пользователя. Это значение выбрано по умолчанию.
     - **sAMAccountName (for Microsoft Active Directory)** – для поиска пользователей в Microsoft Active Directory. Атрибутом может быть пре-Windows 2000 имя пользователя (англ. pre-Windows 2000 logon name).
   - В поле **Bind DN** введите учетную запись на LDAP-сервере, которую оркестратор должен использовать для поиска учетных записей пользователей. Поддерживаются два формата значения:
     - OpenLDAP – uid=ldap_search,ou=system.
     - Microsoft Active Directory – CN=ldap_search,OU=user_group,DC=company,DC=com.
   - В поле **Bind password** введите пароль учетной записи на LDAP-сервере.

4. При необходимости нажмите на кнопку **Проверка аутентификации**, чтобы убедиться в доступности LDAP-сервера.

5. Нажмите на кнопку **Сохранить**.

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

Вы можете выполнить одно из следующих действий с подключением к LDAP-серверу, нажав сначала на него, затем на кнопку **Управление** и выбрав соответствующее значение в раскрывающемся списке:

- Удалить подключение к LDAP-серверу, выбрав **Удалить**.
- Изменить указанный в параметрах подключения к LDAP-серверу пароль, выбрав **Изменить пароль**.

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. На странице настройки пользователей выберите вкладку **Права доступа**.
2. Нажмите на кнопку **+ Новое разрешение**.
3. В отобразившейся области настройки настройте параметры прав доступа, выполнив следующие действия:
   - В поле **Имя** введите имя права доступа. Максимальная длина: 250 символов.
   - В блоке **Доступ к ресурсам** укажите уровень доступа пользователей к разделам и подразделам веб-интерфейса оркестратора. Существуют следующие уровни доступа:
     - **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 установить флажок **Распространить** рядом с разделом/подразделом, чтобы предоставить выбранный уровень доступа ко всем его подразделам. По умолчанию флажок снят.
4. Нажмите на кнопку **Сохранить**.

Право доступа отобразится в таблице. Теперь при создании пользователей им можно назначать созданное право доступа.

Вы можете выполнить одно из следующих действий с правом доступа, нажав сначала на него, затем на кнопку **Управление** и выбрав соответствующее значение в раскрывающемся списке:

- Удалить право доступа, выбрав **Удалить**.
- Копировать право доступа, выбрав **Копировать**.

Создание пользователя

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

Чтобы создать пользователя:

1. На странице настройки пользователей нажмите на кнопку **+ Новый пользователь**.

2. В отобразившейся области настройки настройте параметры пользователя, выполнив следующие действия:

   - В раскрывающемся списке **Источник** выберите тип авторизации пользователя:

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

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

   - 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.

   - 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 .

   - В раскрывающемся списке **Роль** выберите одно из следующих значений:

     - **Администратор** – пользователь имеет доступ ко всему решению.

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

   - В раскрывающемся списке **Права доступа** выберите право доступа для пользователя.

   - Установите флажок **Требуется подтверждение запроса**, чтобы для выполнения любого действия пользователя требовалось подтверждение администратора. Если флажок снят, пользователь может свободно вносить любые изменения в параметры компонентов решения. По умолчанию флажок снят.

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

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

   - В поле **Email** введите адрес электронной почты пользователя.

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

3. Нажмите на кнопку **Сохранить**.

Пользователь отобразится в таблице. Вы можете выполнить одно из следующих действий с пользователем, нажав сначала на него, затем на кнопку **Управление** и выбрав соответствующее значение в раскрывающемся списке:

- Удалить пользователя, выбрав **Удалить**.
- Активировать или заблокировать пользователя, выбрав **Активировать** или **Заблокировать**. Вам нужно активировать пользователя после создания. Заблокированные пользователи не могут авторизоваться в веб-интерфейсе оркестратора.
- Изменить пароль пользователя, выбрав **Изменить пароль**.

Создание группы пользователей

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

Перед выполнением этой инструкции требуется выполнить следующие действия:

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

Чтобы создать группу пользователей:

1. На странице настройки пользователей выберите вкладку **Группы**.
2. Нажмите на кнопку **+ Новая группа**.
3. В отобразившейся области настройки настройте параметры группы пользователей, выполнив следующие действия:
   - В поле **Имя** введите имя группы пользователей на LDAP-сервере в формате user@domain или domain\user.
   - В раскрывающемся списке **Роль** выберите одно из следующих значений:
     - **Администратор** – пользователи в группе имеют доступ ко всему решению.
     - **Тенант** – пользователи в группе имеют доступ только к тенанту, которому вы ее назначаете.
   - В раскрывающемся списке **Права доступа** выберите право доступа для группы пользователей.
4. Нажмите на кнопку **Сохранить**.

Группа пользователей отобразится в таблице. Вы можете удалить группу пользователей, нажав сначала на нее, затем на кнопку **Управление** и выбрав **Удалить** в раскрывающемся списке.

Работа с 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. Как правило, экземпляр SD-WAN настаивается в соответствии с требованиями конкретной организации для обеспечения необходимых уровней гибкости, безопасности и производительности при передачи данных через WAN-сеть. Вы можете просматривать конфигурацию экземпляра SD-WAN, а также выполнять его настройку.

Клиент вашей организации, которому выделяется логический набор сетевых и/или вычислительных ресурсов, для построения сети SD-WAN.

При развертывании экземпляра SD-WAN вы применяете к нему шаблон экземпляра SD-WAN. Параметры развернутого решения настраиваются в соответствии с примененным шаблоном. Определенные параметры отдельного экземпляра SD-WAN можно изменить, если они не соответствуют вашим требованиям.

Шаблон экземпляра SD-WAN

Шаблоны экземпляров SD-WAN используются для централизованной настройки параметров экземпляров SD-WAN. Вы можете указать все необходимые 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.

Клиент вашей организации, которому выделяется логический набор сетевых и/или вычислительных ресурсов, для построения сети SD-WAN.

В шаблон экземпляра SD-WAN требуется добавить тенантов, для которых он будет использоваться. При развертывании экземпляр SD-WAN каждого из этих тенантов получает параметры из используемого шаблона.

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 будет развернуто. 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.

Создание шаблона экземпляра SD-WAN

Чтобы создать шаблон экземпляра SD-WAN:

1. В навигационной панели перейдите в раздел **SD-WAN**.
2. Нажмите на кнопку **+ Шаблон экземпляра SD-WAN**.

Откроется подраздел **Шаблоны экземпляров SD-WAN**, и в нем отобразится шаблон. По умолчанию ему присваивается имя в формате Template <порядковый номер шаблона>.

Вы можете выполнить одно из следующих действий с шаблоном экземпляра SD-WAN, нажав сначала на него, затем на соответствующую кнопку в блоке **Действия** вверху справа:

- Удалить шаблон экземпляра SD-WAN, нажав на кнопку **Удалить**.
- Сделать шаблон экземпляра SD-WAN шаблоном по умолчанию, нажав на кнопку **Назначить шаблоном по умолчанию**.

Добавление тенанта в шаблон экземпляра SD-WAN

Перед выполнением этой инструкции требуется создать тенанта.

Чтобы добавить тенанта в шаблон экземпляра SD-WAN:

1. В области настройки шаблона экземпляра SD-WAN выберите вкладку **Тенанты**.
2. Нажмите на кнопку **+ Добавить тенанта**.
3. В открывшемся окне выберите тенанта, которого требуется добавить и нажмите на кнопку **Применить**.

   Тенант отобразится в таблице. Вы можете удалить тенанта из шаблона, нажав на кнопку **Удалить** рядом с ним в столбце **Действия**.
4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Настройка высокой доступности (high availability)

Архитектура решения предоставляет возможность сохранения высокой доступности (англ. high availability) экземпляров SD-WAN в случае возникновения следующих аварий:

- прекращение работы или перегрузка виртуальных машин;
- прекращение работы устройств CPE;
- прекращение работы 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 области настройки шаблона экземпляра SD-WAN выберите вкладку **Высокая доступность**.

2. Выберите количество узлов контроллера SD-WAN, которое требуется использовать при развертывании экземпляра SD-WAN.

3. Вверху справа 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 области настройки шаблона экземпляра SD-WAN выберите вкладку **Транспортная/сервисная стратегия**.

2. Убедитесь, что в раскрывающемся списке выбрана транспортная стратегия **B4N Generic VNI Swapping Transport**.

Действия с экземпляром SD-WAN

После развертывания экземпляра SD-WAN для тенанта вы можете выполнять с ним действия, которые отображаются в соответствующем блоке.

Чтобы выполнить требуемое действие с экземпляром SD-WAN,

в области настройки экземпляра SD-WAN в блоке **Действия** нажмите на одну из следующих кнопок:

- **Удалить** – удалить экземпляр SD-WAN, все назначенные ему устройства CPE, а также сетевой сервис, в котором он был развернут. Альтернативным способом удаления экземпляра является удаление сетевого сервиса, в котором он был развернут.

- **Показать связанные устройства CPE** – отобразить список устройств CPE, назначенных выбранному экземпляру SD-WAN.

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.

Чтобы добавить тенанта в экземпляр SD-WAN:

1. В области настройки экземпляра SD-WAN выберите вкладку **Самообслуживание тенантов**.

2. Нажмите на кнопку **+ Добавить**.

3. В открывшемся окне выберите тенанта, которого требуется добавить в экземпляр SD-WAN, и в поле **Максимум CPE** введите максимальное количество доступных для него устройств.

4. Нажмите на кнопку **Сохранить**.

Тенант отобразится в таблице. Вы можете удалить тенанта из экземпляра, нажав на кнопку **Удалить** рядом с ним в столбце **Действия**.

Создание пула экземпляров SD-WAN

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).

Чтобы создать пул экземпляров SD-WAN:

1. В навигационной панели перейдите в раздел **SD-WAN**.

2. Нажмите на кнопку **+ Пул экземпляров SD-WAN**.

3. В открывшемся окне укажите имя пула экземпляров SD-WAN и нажмите на кнопку **Добавить**.

   Откроется подраздел **Пулы экземпляров SD-WAN**, и пул отобразится в таблице. Теперь в него необходимо добавить экземпляры SD-WAN. Вы можете удалить пул, нажав сначала на него, затем на кнопку **Удалить** в блоке **Действия**.

4. Нажмите на созданный пул экземпляров SD-WAN и выберите вкладку **Экземпляры SD-WAN**.

5. Нажмите на кнопку **+ Добавить экземпляр SD-WAN**.

6. В открывшемся окне выберите экземпляр SD-WAN, который требуется добавить в пул.

7. Нажмите на кнопку **Добавить**.

   Экземпляр SD-WAN отобразится в таблице. Вы можете удалить экземпляр из пула SD-WAN, нажав на кнопку **Удалить** рядом с ним в столбце **Действия**.

8. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию пула экземпляров SD-WAN.

Работа с 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 или Arm/MIPS;
- отсутствие зависимости от определенных производителей;
- минимальные характеристики аппаратных ресурсов, таких как процессор и операционная память.

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.

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

  Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

- **Universal CPE** (далее также uCPE) – локальное размещение VNF улучшает время отклика, оптимизирует транспортные потоки и сохраняет возможность управлять этими VNF через веб-интерфейс оркестратора.

  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.

Состав устройств CPE

Устройства CPE имеют следующие внешние интерфейсы:

- Один или несколько LAN-интерфейсов. Вы можете объединить несколько LAN-интерфейсов в коммутатор с помощью Linux-мостов для выполнения следующих задач:
  - Увеличение пропускной способности – объединение нескольких LAN-интерфейсов позволяет быстрее передавать данные на подключенные к коммутатору сетевые устройства. Это особенно актуально для сценариев, когда по сети передается большое количество трафика или при подключении нескольких устройств с высокими требованиями к пропускной способности, таких как серверы или системы хранения данных.
  - Балансировка нагрузки – трафик можно распределять между объединенными LAN-интерфейсами для оптимизации использования сетевых ресурсов и предотвращения появления узких мест (англ. bottlenecks). Это повышает общую производительность сети.

- Обеспечение высокой доступности – наличие нескольких LAN-интерфейсов подразумевает резервирование каждого из них, так как при отказе одного интерфейса трафик может быть передан на другой сохранивший свою работоспособность интерфейс. Это позволяет свести количество перерывов в работе сети до минимума.

- Упрощение процесса управления сетью – объединенными LAN-интерфейсы можно управлять централизованно без необходимости настраивать каждый индивидуальный интерфейс.

- Упрощение процесса масштабирования сети – добавление новых LAN-интерфейсов в уже существующий коммутатор позволяет расширять вашу сеть без необходимости в длительной перенастройке.

- 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:

> Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

- 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.

  > Инструмент управления, мониторинга и диагностики сети SD-WAN, также отвечающий за виртуализацию сетевых функций (англ. Network Function Virtualization, NFV). Для управления оркестратором используется графический веб-интерфейс.

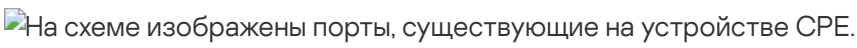
- 2 (ovs-lan) – обеспечивает подключение к Linux-мосту.

- 4800–4803 – для каждого WAN-интерфейса SD-WAN создается GENEVE-интерфейс. 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.

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

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.

Менеджер, обеспечивающий управление и мониторинг вычислительных и сетевых ресурсов, а также ресурсов хранения в виртуальной инфраструктуре. С его помощью VNF взаимодействуют со всеми этими ресурсами.

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.

Клиент вашей организации, которому выделяется логический набор сетевых и/или вычислительных ресурсов, для построения сети SD-WAN.

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.

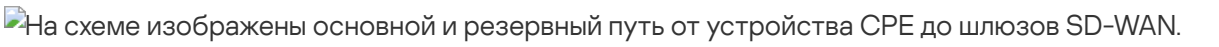
Логическая схема устройства uCPE

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**.

Контролирует передачу пакетов трафика по сети через устройства CPE. В плоскость управления трафиком входят оркестратор и контроллер SD-WAN.

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.

Инструмент конфигурации VNF, развернутых оркестратором.

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

Каждое устройство CPE может иметь один из следующих статусов:

- *Неизвестно* – устройство подключено к оркестратору, но для него не создана запись в подразделе **Устройства CPE**.
- *Ожидание* – для устройства создана запись в подразделе **Устройства CPE**, 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.

Также устройства CPE могут находиться в следующих состояниях:

- *Активировано* – устройство создано и к нему применена конфигурация назначенного шаблона. Вы можете подключить такое устройство к транспортным сервисам и использовать его для передачи трафика.
- *Деактивировано* (в статусе *Ожидание*) – устройство создано, но к нему 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.

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.

> Контролирует передачу пакетов трафика по сети через устройства CPE. В плоскость управления трафиком входят оркестратор и контроллер 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.

Создание шаблона 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. При необходимости конфигурацию можно изменить локально на устройстве даже после применения шаблона

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.

Чтобы создать шаблон CPE:

1. В навигационной панели перейдите в раздел **SD-WAN**.
2. Нажмите на кнопку **+ Шаблон CPE**.
3. В открывшемся окне настройте параметры шаблона CPE, выполнив следующие действия:
   - В поле **Имя** введите имя шаблона CPE.
   - В раскрывающемся списке **Тип** выберите тип шаблона CPE:
     - **CPE** – шаблон **стандартного устройства CPE**. Это значение выбрано по умолчанию.

       Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

     - **uCPE** – шаблон устройства **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.
4. Нажмите на кнопку **Добавить**.

Откроется подраздел **Шаблоны CPE**, и в нем отобразится шаблон. Теперь его можно применить к требуемым устройствам.

Вы можете выполнить одно из следующих действий с шаблоном CPE, нажав сначала на него, затем на соответствующую кнопку в блоке **Действия** вверху справа:

- Удалить шаблон CPE, нажав на кнопку **Удалить**. Вы не можете удалить шаблон, который применен к устройствам CPE.

- Импортировать в шаблон CPE конфигурацию другого шаблона, нажав на кнопку **Импортировать**. Вы можете выбрать определенные вкладки шаблона, чтобы изменить указанные на них параметры в соответствии с импортируемой конфигурацией. Параметры, указанные на не выбранных вкладках, не изменятся. Для импорта требуется указать путь к архиву с конфигурацией.

  Шаблон CPE останется примененным к устройствам, но конфигурация этих устройств не изменяется автоматически в соответствии с указанным архивом.

- Экспортировать конфигурацию шаблона CPE, нажав на кнопку **Экспортировать**. На ваше локальное устройство сохранится архив в формате TAR.GZ, который 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.

- Клонировать шаблон CPE, нажав на кнопку **Копировать**. Клонированный шаблон не будет применен ни к одному устройству CPE.
- Экспортировать параметры подключения устройства к сети SD-WAN, а также конфигурацию интерфейсов SD-WAN, нажав на кнопку **Экспортировать параметры SD-WAN**. На ваше локальное устройство сохранится файл в формате JSON с именем <Имя шаблона>sdwan-config.
- Экспортировать конфигурацию сетевых интерфейсов, нажав на кнопку **Экспортировать сетевые интерфейсы**. На ваше локальное устройство сохранится файл в формате JSON и именем <Имя шаблона>-network-config.
- Отобразить список устройств, к которым применен шаблон CPE, нажав на кнопку **Показать связанные устройства CPE**.

Решение типовых задач с устройством CPE

После завершения работы с шаблоном CPE вы можете перейти к созданию и настройке отдельных устройств. При создании устройства к нему необходимо применить шаблон. Конфигурация устройства настраивается в соответствии с примененным шаблоном, однако в нее можно внести локальные изменения, если не все параметры соответствуют вашим требованиям.

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 создавать устройства CPE в разделе **Тенанты**, а также подразделах **Устройства CPE** и **Экземпляры SD-WAN** веб-интерфейса оркестратора.

Чтобы создать устройство CPE:

1. Откройте окно создания устройства CPE, выполнив одно из следующих действий:

   - В разделе управления тенантами в блоке **Тенанты** выберите требуемого тенанта и в блоке **Устройства CPE** нажмите на кнопку **+ Устройство CPE**.
   - В навигационной панели перейдите в раздел **SD-WAN** и нажмите на кнопку **+ Устройство CPE**.
   - В области настройки экземпляра SD-WAN нажмите на кнопку **Добавить устройство CPE**.

2. В открывшемся окне, настройте параметры устройства CPE, выполнив следующие действия:

   - В поле **Имя** введите имя устройства CPE.
   - В поле **DPID** введите идентификатор DPID устройства CPE.
   - В раскрывающемся списке **Установить 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.
   - В поле **Описание** введите краткое описание устройства.
   - В блоке **Тенант** выберите основного тенанта. Вы также можете выбрать пул экземпляров SD-WAN или отдельный экземпляр из пула. Если вы создаете устройство в разделе **Тенанты**, значение в блоке выбирается автоматически.
   - В блоке **Клиентский тенант** выберите тенанта организации вашего клиента.
   - В блоке **Шаблон UNI** выберите шаблон UNI, который требуется применить к устройству.
   - В блоке **Шаблон CPE** выберите шаблон CPE, который требуется применить к устройству.

3. Нажмите на кнопку **Далее** и в поле **Адрес** укажите почтовый адрес площадки устройства CPE. По мере ввода адреса вам предлагается выбрать адрес в раскрывающемся списке.

   Адрес отобразится на карте.

4. Нажмите на кнопку **Добавить устройство CPE**.

Вы получите один из следующих результатов:

- Если вы создали устройство в разделе **Тенанты**, оно отобразится в блоке **Устройства CPE**.
- Если вы создали устройство в подразделе **Устройства CPE**, оно отобразится в этом подразделе.
- Если вы создали устройство в подразделе **Экземпляры SD-WAN**, в новой вкладке браузера откроется веб-интерфейс экземпляра SD-WAN. Вы будете автоматически авторизованы как администратор

тенанта.

Теперь созданное устройство CPE можно настроить, после чего использовать для передачи трафика.

Вы можете выполнить одно из следующих действий с устройством CPE, нажав сначала на него, затем на соответствующую кнопку в блоке **Действия** вверху справа:

- Удалить устройство CPE, нажав на кнопку **Удалить**.
- Изменить адрес площадки устройства CPE, нажав на кнопку **Указать адрес**.
- Активировать или деактивировать устройство CPE, нажав на кнопку **Активировать** или **Деактивировать**. При активации устройства к нему применяется конфигурация шаблона CPE. Не активированное устройство невозможно использовать для передачи трафика.
- Просмотреть пароль устройства CPE, нажав на кнопку **Показать пароль**.
- Отобразить URL для активации устройства CPE, нажав на кнопку **Получить URL активации**.
- Зарегистрировать устройство CPE или отменить его регистрацию, нажав на кнопку **Зарегистрировать** или **Отменить регистрацию**. Кнопка **Зарегистрировать** отображается только для устройств, которые подключились к оркестратору и не были сопоставлены ни с одной из созданных записей.
- Подключиться к консоли устройства CPE по протоколу SSH, нажав на кнопку **Открыть SSH-консоль**. В новой вкладке веб-браузера откроется окно консоли.
- Подключиться к веб-консоли устройства CPE, нажав на кнопку **Открыть веб-консоль**. В новой вкладке веб-браузера откроется окно консоли и вам потребуется выполнить авторизацию.
- Запустить все добавленные на устройстве CPE скрипты, нажав на кнопку **Запустить скрипты**.
- Перезагрузить устройство CPE, нажав на кнопку **Перезагрузить**.
- Выключить устройство CPE, нажав на кнопку **Выключить**. При выключении в оперативную систему устройства CPE отправляется команда `shutdown`.
- Экспортировать параметры подключения устройства CPE к сети SD-WAN, а также конфигурацию интерфейсов SD-WAN, нажав на кнопку **Экспортировать параметры SD-WAN**. На ваше локальное устройство сохранится файл в формате JSON с именем <Имя устройства>sdwan-config.
- Экспортировать конфигурацию сетевых интерфейсов, нажав на кнопку **Экспортировать параметры SD-WAN**. На ваше локальное устройство сохранится файл в формате JSON и именем <Имя устройства>-network-config.

Регистрация устройства CPE

Если устройство CPE подключается к оркестратору и не может быть сопоставлено ни с одной из созданных вами записей, его нужно зарегистрировать.

Чтобы зарегистрировать устройство CPE:

1. В области настройки устройства CPE в блоке **Действия** нажмите на кнопку **Зарегистрировать**.
2. В открывшемся окне настройте параметры устройства CPE, выполнив следующие действия:

- В раскрывающемся списке **Установить 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.
- В поле **Описание** введите краткое описание устройства.
- В блоке **Тенант** выберите основного тенанта. Вы также можете выбрать пул экземпляров SD-WAN или отдельный экземпляр из пула. Если вы создаете устройство в разделе **Тенанты**, значение в блоке выбирается автоматически.
- В блоке **Клиентский тенант** выберите тенанта организации вашего клиента.
- В блоке **Шаблон UNI** выберите шаблон UNI, который требуется применить к устройству.
- В блоке **Шаблон CPE** выберите шаблон CPE, который требуется применить к устройству.

3. Нажмите на кнопку **Далее** и в поле **Адрес** укажите почтовый адрес площадки устройства CPE. По мере ввода адреса вам предлагается выбрать адрес в раскрывающемся списке.

   Адрес отобразится на карте.

4. Нажмите на кнопку **Зарегистрировать**.

Статус устройства CPE изменится сначала на *Регистрация*, затем на *Зарегистрировано*.

Ваши дальнейшие действия определяются значением, выбранным в раскрывающемся списке **Установить 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 устройства CPE с помощью URL

Kaspersky SD-WAN поддерживает активацию устройств CPE с помощью URL (англ. URL-based ZTP). Активация с помощью URL упрощает и ускоряет первоначальную настройку CPE путем автоматизации передачи параметров конфигурации в URL и последующего ее применения.

Минимизация ручного вмешательства при активации с помощью URL 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).

> Инструмент управления, мониторинга и диагностики сети SD-WAN, также отвечающий за виртуализацию сетевых функций (англ. Network Function Virtualization, NFV). Для управления оркестратором используется графический веб-интерфейс.

Существуют следующие особенности активации с помощью URL:

- Активация с помощью URL доступна для устройств CPE с прошивкой в стартовом состоянии.
- Устройства CPE не должно находиться в статусе *Неизвестно*.

Вы можете указать шаблон URL для активации при настройке подключения устройства CPE к сети SD-WAN в поле **URL ZTP**.

Чтобы активировать устройство CPE с помощью URL:

1. В области настройки устройства CPE в блоке **Действия** нажмите на кнопку **Получить URL активации** и скопируйте URL.
2. Отправьте URL пользователю, который активирует и настраивает устройство CPE на месте его установки.
3. Для активации устройства CPE пользователю необходимо выполнить следующие действия:
   a. Подключиться к LAN-интерфейсу устройства CPE и получить IP-адрес по DHCP.
   b. Перейти по полученной ссылке или вставить URL в адресную строку браузера.
   c. Дождаться, пока устройство CPE получит конфигурацию, применит полученные параметры и перезагрузится.

Автоматическое удаление и деактивация устройства CPE

Вы можете указать в шаблоне CPE или на отдельном устройстве время, по прошествии которого устройство будет удалено или деактивировано в случае потери связи с **контроллером SD-WAN**.

> Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

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.

Чтобы включить функции автоматического удаления и деактивации устройства CPE:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Деактивация**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.
3. Установите флажок **Включить** рядом с полем **Тайм-аут удаления (мин.)** и укажите в нем время, по прошествии которого устройство CPE требуется удалить при отсутствии связи с контроллером SD-WAN. По умолчанию флажок снят.

   Время указывается в минутах. Диапазон значений: от 1 до 525600. Введенное значение не должно быть ниже значения, которое вы указываете для функции автоматической деактивации.

4. Установите флажок **Включить** рядом с полем **Тайм-аут деактивации (мин.)** и укажите в нем время, по прошествии которого устройство CPE требуется деактивировать при отсутствии связи с контроллером SD-WAN. По умолчанию флажок снят.

   Время указывается в минутах. Диапазон значений: от 1 до 525600. Введенное значение не должно быть выше значения, которое вы указываете для функции автоматического удаления.

5. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства 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 области настройки устройства CPE выберите вкладку **Активация**.

2. В раскрывающемся списке **Двухфакторная аутентификация** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

3. Если вы включили двухфакторную аутентификацию, нажмите на кнопку **Сгенерировать** под полем **Токен**, чтобы сгенерировать ключ безопасности.

4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

5. Введите сгенерированный ключ безопасности на устройстве CPE в папке /etc/config/sdwan.

Установка сертификата оркестратора на устройствах CPE

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.

Чтобы добавить публичный корневой сертификат оркестратора для установки на устройствах CPE:

1. В навигационной панели перейдите в раздел **SD-WAN**.

2. Нажмите на кнопку **+ Сертификат**.

3. Укажите путь к файлу сертификата в формате PEM. Максимальный размер файла: 128 КБ.

Информация о добавленном сертификате отобразится в подразделе **Сертификат**.

4. Если вы хотите принудительно распространить сертификат на устройства CPE, не дожидаясь автоматического распространения сертификата, нажмите на кнопку **Применить к CPE**.

При каждой загрузке нового сертификата в веб-интерфейсе оркестратора сертификат распространяется на устройства CPE автоматически.

При первоначальной активации устройства CPE с помощью URL загруженный в оркестратор сертификат автоматически устанавливается на устройстве.

За 30 дней до окончания срока действия сертификата оркестратор начинает выводить уведомление об этом при каждой авторизации пользователя в веб-интерфейсе оркестратора.

Назначение тегов

Теги – это метки, которые описывают различные параметры устройства CPE, например модель, версию программного обеспечения или адрес расположения. Теги классифицируют устройства для решения 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.

При необходимости 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.

Чтобы назначить тег устройству CPE:

1. Перейдите к назначению тегов, выполнив одно из следующих действий:

   - Если вы хотите назначить тег отдельному устройству CPE, в области настройки этого устройства выберите вкладку **Теги**.

   - Если вы хотите назначить тег нескольким устройствам CPE, в навигационной панели перейдите в раздел **SD-WAN**, установите флажки рядом с требуемыми устройствами и вверху справа в раскрывающемся списке **Действия** выберите **Добавить теги**.

2. Введите тег и нажмите на кнопку добавления кнопка в виде знака плюс.

3. Выполните одно из следующих действий:

   - Если вы назначили тег отдельному устройству CPE, нажмите на кнопку **Сохранить**, чтобы сохранить его конфигурацию.

   - Если вы назначили тег нескольким устройствам, нажмите на кнопку **Добавить**.

Вы можете удалить назначенный тег, нажав на кнопку удаления рядом с ним.

Внеполосное управление устройствами CPE

В основном 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.

Инструмент управления, мониторинга и диагностики сети SD-WAN, также отвечающий за виртуализацию сетевых функций (англ. Network Function Virtualization, NFV). Для управления оркестратором используется графический веб-интерфейс.

Таким образом, 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**.

Когда вы вносите изменения в конфигурацию устройства CPE в веб-интерфейсе оркестратора, он сохраняет новую конфигурацию со статусом *Ожидание*. В свою очередь устройство получает эту конфигурацию при очередном отправлении API-запроса и сообщает об ее успешном применении оркестратору. В этом случае конфигурация 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,

откройте область настройки устройства CPE, на котором требуется просмотреть статус конфигураций.

Конфигурации и их статус отобразятся в таблице **Out of Band Management**.

Работа со скриптами

Скрипт – это последовательность команд и инструкций, которые используются для настройки устройств CPE. Каждый скрипт изменяет один или несколько параметров устройства.

Вы можете добавлять 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.

Инструмент конфигурации VNF, развернутых оркестратором.

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. Вам нужно указать в шаблоне CPE имя и пароль существующего на устройстве пользователя, от имени которого VNFM будет запускать скрипты. Кроме того, для подключения VNFM к консоли устройства требуется указать номер SSH-порта.

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 области настройки шаблона CPE выберите вкладку **Скрипты**.
2. В открывшемся окне настройте параметры подключения VNFM к устройству CPE, выполнив следующие действия:
   - В поле **Имя пользователя по умолчанию** введите имя пользователя для авторизации VNFM в консоли устройства. Максимальная длина: 255 символов.
   - В поле **SSH-порт** введите номер порта для подключения VNFM к консоли устройства CPE. По умолчанию указано значение `1`.
   - В поле **Пароль по умолчанию** введите пароль пользователя для авторизации VNFM в консоли устройства CPE. Максимальная длина: 255 символов. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра .
3. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Добавление скрипта

Вам нужно добавить созданный скрипт в шаблон CPE, чтобы затем он автоматически добавлялся на всех использующих этот шаблон устройствах. Перед выполнением этой инструкции требуется настроить подключение VNFM к консоли устройства CPE.

Чтобы добавить скрипт:

1. В области настройки шаблона CPE выберите вкладку **Скрипты**.
2. Нажмите на кнопку **+ Добавить скрипт**.
3. В открывшемся окне настройте параметры скрипта, выполнив следующие действия:
   - В поле **Имя** введите имя скрипта. Максимальная длина: 255 символов.
   - В поле **Тайм-аут (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`.
   - В раскрывающемся списке **Исполнитель скрипта** выберите одно из следующих значений:

- **Ansible** – это значение выбрано по умолчанию.
- **Shell**.
- **Expect**.
- **Пользовательский** – использовать собственный интерпретатор в VNFM. При выборе этого значения вам нужно ввести путь к интерпретатору в поле **Пользовательский интерпретатор**.

  Инструмент конфигурации VNF, развернутых оркестратором.

- В раскрывающемся списке **Стадия** выберите стадию работы устройства CPE, на которой требуется запускать скрипт:
  - **Регистрация** – это значение выбрано по умолчанию.
  - **Удаление**.
  - **Вручную**– запускать скрипт только вручную.
- В раскрывающемся списке **Авторизация** выберите метод авторизации VNFM в консоли устройства CPE:
  - **SSH-ключ** – VNFM использует SSH-ключ. Это значение выбрано по умолчанию. На устройстве необходимо разместить публичную часть SSH-ключа оркестратора, чтобы авторизация прошла успешно. Для этого вам нужно поместить специально созданный специалистами "Лаборатории Касперского" **скрипт** в файл в формате YML после чего добавить этот файл в шаблон CPE.

    ```
    ---
    - hosts: ${target}
      gather_facts: no
      tasks:
        - name: setting up ssh key
          raw: echo ${ssh.key.public} >> /etc/dropbear/authorized_keys
    ```

  - **Пароль** – VNFM использует имя пользователя и пароль, которые вы указали при настройке подключения VNFM к консоли устройства CPE.
- Установите флажок **Повторный запуск**, чтобы запускать скрипт каждый раз при перезагрузке устройства CPE. По умолчанию флажок снят.
- В поле **Скрипт** укажите путь к файлу со скриптом или к файлу-сценарию Ansible playbook.
- При необходимости в поле **Файл** укажите путь к дополнительным файлам, необходимым для выполнения скрипта. Поддерживаемые форматы архивов с файлами: TAR.GZ и ZIP.

4. Нажмите на кнопку **Сохранить**.

   Скрипт отобразится в таблице со скриптами. Вы можете выполнить одно из следующих действий со скриптом, нажав на соответствующую кнопку рядом с ним в столбце **Действия**:

   - Изменить параметры скрипта, нажав на кнопку **Изменить**.
   - Удалить скрипт, нажав на кнопку **Удалить**.
   - Запустить скрипт вручную, нажав на кнопку **Запустить скрипт**.

- Просмотреть содержимое скрипта, нажав на кнопку **Просмотреть скрипт**.

5. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Настройка порядка запуска скриптов

Порядок запуска скриптов используется, когда на устройстве CPE требуется одновременно автоматически запустить несколько скриптов. Например, если вы добавили два скрипта и каждый из них автоматически запускается при регистрации устройства, порядок запуска определяет, какой из них будет запущен первым. По умолчанию при автоматическом запуске первым запускается скрипт, который был добавлен раньше всех остальных.

Вы можете настроить порядок запуска скриптов в шаблоне CPE или на отдельном устройстве.

Чтобы настроить порядок запуска скриптов:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Скрипты**.
2. Настройте порядок выполнения скриптов с помощью кнопок **Вниз** и **Вверх** в столбце **Порядок запуска** рядом с каждым скриптом. Скрипт, который находится вверху, будет запущен первым.
3. Нажмите на кнопку **Применить**.
4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Запуск скрипта вручную

Для запуска скрипта его необходимо добавить в шаблон CPE, после чего он будет автоматически добавлен на всех использующих шаблон устройствах. При добавлении скрипта вы выбираете, будет ли он запускаться автоматически или вручную. Любой скрипт можно запустить вручную, не дожидаясь автоматического запуска.

Вы можете вручную запустить скрипт в шаблоне CPE или на отдельном устройстве, а также создать задачу по отложенному запуску скрипта.

Чтобы запустить скрипт вручную:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Скрипты**.
2. Нажмите на кнопку **Запустить скрипт** рядом со скриптом, который требуется запустить.
3. Если вы запускаете скрипт в шаблоне CPE, выполните следующие действия:

   a. В открывшемся окне в раскрывающемся списке выберите, на каких устройствах требуется запустить скрипт:

      - **Запустить скрипт на всех связанных устройствах CPE** – запустить скрипт на всех использующих шаблон устройствах CPE. Это значение выбрано по умолчанию.

- **Запустить скрипт на всех связанных устройствах CPE с указанными тегами** – запустить скрипт на использующих шаблон устройствах CPE с определенными тегами. При выборе этого значения вам ввести теги в поле снизу.

b. Нажмите на кнопку **Применить**.

4. Если вы запускаете скрипт на отдельном устройстве CPE, в открывшемся окне нажмите на кнопку **Запустить скрипт**.

В зависимости от выполненных вами действий скрипт будет запущен:

- на выбранном устройстве CPE;
- на всех устройствах, использующих выбранный шаблон CPE;
- на устройствах с указанными тегами, использующих выбранный шаблон CPE.

Для запуска всех скриптов вы можете нажать на кнопку **Запустить скрипты** в блоке **Действия**. Шаги для запуска всех скриптов не отличаются от шагов для запуска отдельного скрипта.

Отложенный запуск скрипта

Для запуска скрипта его необходимо добавить в шаблон CPE, после чего он будет автоматически добавлен на всех использующих шаблон устройствах. При добавлении скрипта вы выбираете, будет ли он запускаться автоматически или вручную. Любой скрипт можно запустить вручную, не дожидаясь автоматического запуска.

Вы можете создать задачу по отложенному запуску скрипта в планировщике задач. При этом если вы хотите запустить скрипт сразу на нескольких устройствах, их необходимо предварительно сгруппировать с помощью тегов.

Чтобы создать задачу по отложенному запуску скрипта в планировщике задач:

1. В навигационной панели перейдите в раздел **Планировщик**.
2. Нажмите на кнопку **+ Отложенная задача**.
3. В открывшемся окне настройте параметры отложенной задачи, выполнив следующие действия:
   - В раскрывающемся списке **Тип** выберите **Отложенный запуск скрипта**.
   - В поле **Имя** введите имя отложенной задачи.
   - В раскрывающемся списке **Выберите скрипты** выберите, каким образом определяются устройства CPE, на которых требуется запустить скрипт:
     - **Все CPE с выбранным шаблоном** – скрипт требуется запустить на всех устройствах, использующих шаблон CPE. Выбрать шаблон вы сможете далее. Это значение выбрано по умолчанию.
     - **Все CPE с выбранным шаблоном и определенными тегами** – скрипт требуется запустить на устройствах, использующих шаблон CPE и имеющих указанные теги. Выбрать шаблон и указать теги вы сможете далее.

- **Определенное CPE с выбранным шаблоном** – скрипт требуется запустить на отдельных устройствах, использующих шаблон CPE. Выбрать шаблон и устройства вы сможете далее.

- В блоках **Шаблон CPE** и **Скрипты** выберите шаблон и скрипт, который требуется запустить.

- В поле **Дата и время выполнения** введите дату и время для выполнения отложенной задачи. По умолчанию указаны дата и время в момент, когда вы начали создавать отложенную задачу.

4. Если в раскрывающемся списке **Выберите скрипты** вы выбрали **Определенное CPE с выбранным шаблоном**, в блоке **CPE** выберите устройства, на которых требуется запустить скрипт.

5. Если в раскрывающемся списке **Выберите скрипты** вы выбрали **Все CPE с выбранным шаблоном и определенными тегами**, в поле **Теги** введите теги устройств, на которых требуется запустить скрипт.

6. Нажмите на кнопку **Добавить**.

Отложенная задача отобразится в таблице. Скрипт будет запущен на устройствах CPE в указанное время.

Вы можете выполнить одно из следующих действий с отложенной задачей, нажав сначала на нее, затем на соответствующую кнопку в блоке **Действия**:

- Выполнить отложенную задачу вручную, нажав на кнопку **Выполнить сейчас**.

- Удалить отложенную задачу, нажав на кнопку **Удалить**.

Настройка подключения устройства CPE к сети SD-WAN

Вам нужно настроить подключение устройства CPE к сети SD-WAN, чтобы обеспечить взаимодействие между ним и **плоскостью управления сетью**. Вы можете сделать это в шаблоне CPE или на отдельном устройстве.

> Контролирует передачу пакетов трафика по сети через устройства CPE. В плоскость управления трафиком входят оркестратор и контроллер SD-WAN.

Обратите внимание, что при настройке подключения на отдельном устройстве CPE невозможно изменить 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 устройства к сети SD-WAN:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры SD-WAN**.

2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Настройте параметры подключения, выполнив следующие действия:

   - В поле **IP/FQDN оркестратора** введите IP-адрес или FQDN оркестратора. Максимальная длина: 50 символов.

   - В раскрывающемся списке **Протокол оркестратора** выберите протокол для подключения устройства CPE к оркестратору:

     - **http**;

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

   - В поле **Порт оркестратора** введите номер порта оркестратора. Диапазон значений: от 0 до 65535.

   - 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.

   - В раскрывающемся списке **Перезагрузить, если контроллеры не доступны** выберите, требуется ли перезагружать устройство CPE при потере связи с контроллером SD-WAN:

     - **Да** – при выборе этого значения вам нужно ввести время в секундах, по прошествии которого устройство CPE будет перезагружено при потере связи с контроллером SD-WAN, в поле **Тайм-аут до перезагрузки**. Диапазон значений: от 60 до 2 073 600.

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

   - В раскрывающемся списке **Приоритетный интерфейс управления** выберите, каким образом выполняется переключение основной сессии для обеспечения взаимодействия устройства CPE с контроллерами SD-WAN:

     - **Random** – 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.

       При выборе этого значения отображается флажок **Обратное переключение**. Если флажок установлен, выполняется обратное переключение на предыдущую сессию при ее восстановлении по истечении указанного вами времени. Вам нужно указать время в секундах для переключения в поле **Тайм-аут**. Если флажок снят, обратное переключение на предыдущую основную сессию не происходит. По умолчанию флажок снят.

   - 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`.

   - В поле **URL ZTP** введите шаблон URL для активации устройства CPE с помощью URL. При вводе шаблона URL 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 URL: `http://192.168.7.1/cgi-bin/luci/config?payload={config}`

4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Интерфейсы устройства CPE

Kaspersky SD-WAN использует следующие типы интерфейсов для передачи трафика между устройствами CPE:

- **Сетевые интерфейсы** – Linux-интерфейсы для установления соединения с внешними физическими устройствами. Вам нужно назначить IP-адрес каждому сетевому интерфейсу по протоколу DHCP или статически.

  При создании сетевого интерфейса вы указываете уникальный псевдоним (англ. alias). Этот псевдоним позже требуется указать при создании интерфейса SD-WAN.

  Например, вы можете создать сетевой интерфейс, которому в последствии будет назначен IPv6-адрес вместе с другими параметрами, такими как MAC-адрес и значение MTU.

- **Интерфейсы SD-WAN** – логические интерфейсы для построения топологии сети SD-WAN. Имеют предопределенные типы и ссылаются на сетевые интерфейсы (сопоставление происходит через псевдоним сетевого интерфейса). При создании интерфейса SD-WAN для него автоматически создается OpenFlow-интерфейс с указанным вами номером.

- **OpenFlow-интерфейсы** – интерфейсы наложенной SDN-сети, которые соответствуют интерфейсам SD-WAN и используются контроллером для управления трафиком в рамках сети SD-WAN. Вы можете создавать UNI и сервисные интерфейсы поверх OpenFlow-интерфейсов.

- **UNI и сервисные интерфейсы** – интерфейсы для подключения к транспортным сервисам. Вы можете создавать эти интерфейсы поверх любых OpenFlow-интерфейсов за исключением тех, которые соответствуют WAN-интерфейсам SD-WAN.

  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**.

  > Клиент вашей организации, которому выделяется логический набор сетевых и/или вычислительных ресурсов, для построения сети SD-WAN.

  Обратите внимание, что при создании UNI для него автоматически создается соответствующий сервисный интерфейс, однако для сервисных интерфейсов не создается UNI.

Создание интерфейса SD-WAN

Вы можете создавать интерфейсы SD-WAN в шаблоне CPE или на отдельном устройстве. Kaspersky SD-WAN временно поддерживает создание только WAN-интерфейсов SD-WAN.

Чтобы создать интерфейс SD-WAN:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры SD-WAN → Интерфейсы**.

2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Нажмите на кнопку **+ Добавить интерфейс**.

4. В открывшемся окне настройте параметры интерфейса SD-WAN, выполнив следующие действия:

   - В поле **OpenFlow-интерфейс** введите номер OpenFlow-интерфейса, который требуется создать на виртуальном коммутаторе устройства CPE.

   - В поле **Интерфейс (псевдоним)** введите псевдоним сетевого интерфейса, с которым требуется связать OpenFlow-интерфейс.

   - В поле **Максимальная скорость** введите максимальную скорость интерфейса SD-WAN в МБит в секунду. Диапазон значений: от 1 до 100000. По умолчанию указано значение `1000`.

   - В поле **IP для отслеживания** введите IP-адрес хоста, доступность которого определяет доступность интерфейса SD-WAN, и нажмите на кнопку **+ Добавить**. Вы можете указать несколько хостов.

   - 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.

   - В поле **Интервал** введите интервал в секундах для проведения тестов интерфейса SD-WAN. Диапазон значений: от 1 до 600. По умолчанию указано значение `2`.

   - 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`.

   - В поле **Тайм-аут** 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`.

   - 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`.

   - 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`.

   - В раскрывающемся списке **Мониторинг скорости** выберите, требуется ли проверять ограничение скорости интерфейса SD-WAN оператором мобильной связи:

     - **Да**.

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

5. При необходимости выберите вкладку **QoS** и настройте очереди трафика для интерфейса SD-WAN, выполнив следующие действия:

   - 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 SD-WAN.

   - В столбце **Минимум Скорость, %** укажите минимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN. Максимальная скорость указывается на вкладке **Глобальные** в поле **Максимальная скорость**. Сумма значений в столбце не должна превышать 100.

   - В столбце **Максимум Скорость**, **%** укажите максимальную скорость передачи трафика для очереди в процентном выражении от максимальной скорости интерфейса SD-WAN. Максимальная скорость указывается на вкладке **Глобальные** в поле **Максимальная скорость**. Параметр используется для того, чтобы трафик очередей с высоким приоритетом постоянно не вытеснял трафик очередей с низким приоритетом.

6. Нажмите на кнопку **Сохранить**.

   Интерфейс SD-WAN отобразится в таблице. Вы можете выполнить одно из следующих действий с интерфейсом SD-WAN, нажав на соответствующую кнопку рядом с ним в столбце **Действия**:

   > Для выполнения действий с интерфейсом SD-WAN на отдельном устройстве вам нужно сначала установить флажок **Переопределить** рядом с ним. Если флажок снят, вы можете только просмотреть конфигурацию интерфейса SD-WAN, нажав на кнопку **Просмотреть**.

   - Изменить параметры интерфейса SD-WAN, нажав на кнопку **Изменить**.

   - Удалить интерфейс SD-WAN, нажав на кнопку **Удалить**. Это действие можно выполнить только в шаблоне CPE.

   - Выключить интерфейс SD-WAN, нажав на кнопку **Выключить**.

7. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание сетевого интерфейса

Вы можете создавать сетевые интерфейсы в шаблоне CPE или на отдельном устройстве. 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 при создании сетевого интерфейса, зависят от выбранного типа.

Чтобы создать сетевой интерфейс:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры сети**.

2. При настройте отдельного устройства CPE выполните следующие действия:

   - Установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке.

   - При необходимости установите флажок **Игнорировать параметры сети**, чтобы не использовать на устройстве сетевые интерфейсы, унаследованные из шаблона CPE.

   По умолчанию оба флажка сняты. Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Нажмите на кнопку **+ Добавить интерфейс**.

4. В открывшемся окне укажите параметры сетевого интерфейса:

   - **Сетевой интерфейс с автоматическим назначением IP-адреса по протоколу DHCP.**

- В поле **Псевдоним** введите псевдоним, на который вы сможете позже 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`.

- 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.

- Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

- В раскрывающемся списке **Протокол** выберите, каким образом сетевому интерфейсу назначается IP-адрес. Для создания сетевого интерфейса с автоматическим назначением IP-адреса по протоколу DHCP выберите **DHCP client**.

- Установите флажок **Автоматическое включение**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE. По умолчанию флажок установлен.

- Установите флажок **Назначать IP, маршут 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 флажок установлен.

- Установите флажок **Использовать маршрут по умолчанию**, чтобы использовать на сетевом интерфейсе маршрут по умолчанию, получаемый по протоколу DHCP. По умолчанию флажок установлен.

- В блоке **DNS-серверы** нажмите на кнопку **+ Добавить** и укажите IP-адрес DNS-сервера, используемого в вашей сети. Вы можете указать несколько серверов.

- В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет MAC-адрес по умолчанию.

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

- 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`.

- **Сетевой интерфейс со статическим IPv4-адресом.**

- В поле **Псевдоним** введите псевдоним, на который вы сможете позже 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`.

- 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.

- Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

- В раскрывающемся списке **Протокол** выберите, каким образом сетевому интерфейсу назначается IP-адрес. Для создания сетевого интерфейса со статическим IPv4-адресом выберите **Static address IPv4**.

- Установите флажок **Автоматическое включение**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE. По умолчанию флажок установлен.

- Установите флажок **Назначать IP, маршут 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 флажок установлен.

- В поле **IPv4-адрес** введите IPv4-адрес сетевого интерфейса. Вы можете ввести несколько адресов через пробел.

- В поле **Маска подсети IPv4** введите маску IPv4-адреса.

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

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

- В блоке **DNS-серверы** нажмите на кнопку **+ Добавить** и укажите IP-адрес DNS-сервера, используемого в вашей сети. Вы можете указать несколько серверов.

- В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет MAC-адрес по умолчанию.

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

- 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`.

- В блоке **DHCP-сервер** в раскрывающемся списке **Тип** выберите режим работы используемого DHCP-сервера:

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

- **Relay** – при выборе этого значения вам нужно указать адрес сервера в поле **IP DHCP-сервера**.
- **Server**.

Если в блоке **DHCP-сервер** вы выбрали **Server**, укажите параметры DHCP-сервера, выполнив следующие действия:

- В поле **Первый IP** введите IP-адрес, с которого требуется начать выдачу адресов клиентам. По умолчанию указано значение `100`.
- В поле **Лимит** введите максимальное количество IP-адресов, которое может быть выдано клиентам. Диапазон значений: от 1 до 250. По умолчанию указано значение `150`.
- 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`.
- В блоке **DHCP-опции** нажмите на кнопку **+ Добавить** и введите имя DHCP-опции. Максимальная длина: 250 символов. Вы можете указать несколько опций.

- Сетевой интерфейс со статическим IPv6-адресом.

- В поле **Псевдоним** введите псевдоним, на который вы сможете позже 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`.

- 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.

- Установите флажок **Мост**, чтобы создать мост из интерфейсов, указанных в поле **Имя интерфейса**. По умолчанию флажок снят.

- В раскрывающемся списке **Протокол** выберите, каким образом сетевому интерфейсу назначается IP-адрес. Для создания сетевого интерфейса со статическим IPv6-адресом выберите **Static address IPv6**.

- Установите флажок **Автоматическое включение**, чтобы автоматически включать сетевой интерфейс одновременно с устройством CPE. По умолчанию флажок установлен.

- Установите флажок **Назначать IP, маршут 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 флажок установлен.

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

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

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

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

- В поле **Суб-префикс DHCPv6** введите длину суб-префикса DHCPv6, который сетевой интерфейс должен назначать клиентам. Максимальная длина: 256 символов.

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

- В блоке **Класс IPv6** нажмите на кнопку **+ Добавить** и введите класс IPv6-префиксов, который будет принимать сетевой интерфейс. Максимальная длина: 256 символов. Вы можете указать несколько классов.

- В блоке **DNS-серверы** нажмите на кнопку **+ Добавить** и укажите IP-адрес DNS-сервера, используемого в вашей сети. Вы можете указать несколько серверов.

- В поле **Переопределить MAC** введите MAC-адрес сетевого интерфейса. Введенное значение заменяет MAC-адрес по умолчанию.

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

- 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`.

- В блоке **DHCP-сервер** в раскрывающемся списке **Тип** выберите режим работы используемого DHCP-сервера:

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

  - **Relay** – при выборе этого значения вам нужно указать адрес сервера в поле **IP DHCP-сервера**.

  - **Server**.

  Если в блоке **DHCP-сервер** вы выбрали **Server**, укажите параметры DHCP-сервера, выполнив следующие действия:

  - В поле **Первый IP** введите IP-адрес, с которого требуется начать выдачу адресов клиентам. По умолчанию указано значение `100`.

  - В поле **Лимит** введите максимальное количество IP-адресов, которое может быть выдано клиентам. Диапазон значений: от 1 до 250. По умолчанию указано значение `150`.

  - 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`.

  - В блоке **DHCP-опции** нажмите на кнопку **+ Добавить** и введите имя DHCP-опции. Максимальная длина: 250 символов. Вы можете указать несколько опций.

- Сетевой интерфейс для подключения к беспроводной сети.

- В поле **Псевдоним** введите псевдоним, на который вы сможете позже 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`.

- В раскрывающемся списке **Протокол** выберите, каким образом сетевому интерфейсу назначается IP-адрес. Для создания сетевого интерфейса для подключения к беспроводной сети выберите **QMI**.

- В поле **Имя QMI** введите имя модема для подключения к сети. Максимальная длина: 30 символов. Например, вы можете ввести `/dev/cdc-wdm0`.

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

- В раскрывающемся списке **Тип аутентификации** выберите, какая аутентификация используется на сетевом интерфейсе:

  - **PAP**.
  - **CHAP**.
  - **BOTH**.
  - **None**.

- 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.

- 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..

- 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.

- В блоке **Режимы** нажмите на кнопку **+ Добавить** и выберите сетевой режим, который используется на сетевом интерфейсе:

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

- **CDMA**.
- **TD-SCDMA**.

Вы можете указать несколько режимов.

- В поле **Профиль подключения** введите индекс профиля подключения, который сетевой интерфейс должен использовать вместо идентификатора APN. Максимальная длина: 30 символов.
- В раскрывающемся списке **IP-стек** выберите, какой IP-стек используется на сетевом интерфейсе:
  - **IP (for IPv4) –** использовать на сетевом интерфейсе стек протокола IPv4. Это значение выбрано по умолчанию.
  - **IPV6 (for IPv6) –** использовать на сетевом интерфейсе стек протокола IPv6.
  - **IPV4V6 (for dual-stack) –** использовать на сетевом интерфейсе двойной стек IPv4 и IPv6.
- Установите флажок **IPv4 через DHCP**, чтобы назначить сетевому интерфейсу IPv4-адрес по протоколу DHCP. Для того, чтобы установить этот флажок одновременно с флажком **IPv6 через DHCP** в раскрывающемся списке **IP-стек** выберите **IPV4V6 (for dual stack)**. По умолчанию флажок установлен.
- Установите флажок **IPv6 через DHCP**, чтобы назначить сетевому интерфейсу IPv6-адрес по протоколу DHCP. Для того, чтобы установить этот флажок одновременно с флажком **IPv4 через DHCP** в раскрывающемся списке **IP-стек** выберите **IPV4V6 (for dual stack)**. По умолчанию флажок снят.
- Установите флажок **Автоподключение**, чтобы автоматически подключать модем к сети. По умолчанию флажок установлен.
- В поле **PLMN** введите идентификатор PLMN оператора связи. Первые три цифры идентификатора PLMN являются кодом страны, а вторые три цифры – кодом мобильной сети.
- В поле **Тайм-аут** 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`.
- В поле **Серийный номер** введите последовательный порт (англ. serial port) модема. Максимальная длина: 50 символов.
- 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`.

5. Нажмите на кнопку **Сохранить**.

   Сетевой интерфейс отобразится в таблице. Вы можете выполнить одно из следующих действий с сетевым интерфейсом, нажав на соответствующую кнопку рядом с ним в столбце **Действия**:

Для выполнения действий с сетевым интерфейсом на отдельном устройстве вам нужно сначала установить флажок **Переопределить** рядом с ним. Если флажок снят, вы можете только просмотреть конфигурацию сетевого интерфейса, нажав на кнопку **Просмотреть**.

- Изменить параметры сетевого интерфейса, нажав на кнопку **Изменить**.
- Удалить сетевой интерфейс, нажав на кнопку **Удалить**. Это действие можно выполнить только в шаблоне CPE.
- Выключить сетевой интерфейс, нажав на кнопку **Выключить**.

6. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание сервисного интерфейса

Вы можете создавать сервисные интерфейсы поверх OpenFlow-интерфейсов. OpenFlow-интерфейсы создаются автоматически и соответствуют интерфейсам SD-WAN.

Чтобы создать сервисный интерфейс:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Сервисные интерфейсы**.
2. В раскрывающихся списках **Коммутатор** и **Порт** выберите требуемое устройство CPE и OpenFlow-интерфейс.
3. Нажмите на кнопку **Добавить сервисный интерфейс**.
4. В открывшемся окне настройте параметры сервисного интерфейса, выполнив следующие действия:
   - В раскрывающемся списке **Тип** выберите тип инкапсуляции на сервисном интерфейсе:
     - **Access** – это значение выбрано по умолчанию.
     - **VLAN** – при выборе этого значения вам нужно ввести внешнюю метку VLAN в поле **VLAN ID**. Диапазон значений: от 1 до 4094.
     - **Q-in-Q** – при выборе этого значения вам нужно ввести внешнюю метку VLAN в поле **VLAN ID** и внутреннюю метку VLAN в поле **Внутренний VLAN ID**. Диапазон значений: от 1 до 4094.
     - **ACL** – используется для создания ACL-интерфейса.
   - В поле **Описание** введите краткое описание сервисного интерфейса.
5. Нажмите на кнопку **Сохранить**.

Сервисный интерфейс отобразится в таблице. Вы можете выполнить одно из следующих действий с сервисным интерфейсом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Удалить сервисный интерфейс, выбрав **Удалить**. Сервисный интерфейс, который используется другими компонентами решения, например транспортными сервисами, удалить невозможно.
- Показать использование сервисного интерфейса, выбрав **Показать использование**.

Создание ACL-интерфейса

ACL-интерфейсы обеспечивают фильтрацию трафика между транспортными сервисами на основании указанных вами ограничений. Так как ACL-интерфейсы создаются поверх сервисных интерфейсов, перед выполнением этой инструкции требуется создать сервисный интерфейс.

Чтобы создать ACL-интерфейс:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Сервисные интерфейсы**.
2. В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-интерфейс, поверх которого создан требуемый сервисный интерфейс.
3. Нажмите на кнопку **Добавить сервисный интерфейс**.
4. В открывшемся окне настройте параметры ACL-интерфейса, выполнив следующие действия:
   - В раскрывающемся списке **Тип** выберите тип инкапсуляции на сервисном интерфейсе. Для создания ACL-интерфейса выберите **ACL**.
   - В раскрывающемся списке **Сервисный интерфейс** выберите сервисный интерфейс, поверх которого требуется создать ACL-интерфейс.
   - В раскрывающемся списке **Фильтр трафика** выберите фильтр трафика для ACL-интерфейса. Вы можете использовать один фильтр трафика для нескольких ACL-интерфейсов.
   - В раскрывающемся списке **Порядковый номер** 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.
   - В поле **Описание** введите краткое описание ACL-интерфейса.
5. Нажмите на кнопку **Сохранить**.

ACL-интерфейс отобразится в таблице. Вы можете выполнить одно из следующих действий с ACL-интерфейсом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Удалить ACL-интерфейс, выбрав **Удалить**. ACL-интерфейс, который используется другими компонентами решения, например транспортными сервисами, удалить невозможно.
- Показать использование ACL-интерфейса, выбрав **Показать использование**.

Создание шаблона UNI

Вы можете создать все необходимые UNI в одном шаблоне, после чего применять его устройствам CPE при первичном создании и регистрации. В этом случае все UNI из шаблона автоматически создаются на устройствах. Таким образом, вам не нужно создавать UNI вручную на каждом отдельном устройстве.

Чтобы создать шаблон UNI:

1. В навигационной панели перейдите в раздел **SD-WAN**.
2. Нажмите на кнопку **+ Шаблон UNI**.
3. В открывшемся окне укажите имя шаблона и нажмите на кнопку **Добавить шаблон UNI**.

   Откроется подраздел **Шаблоны UNI**, и шаблон отобразится в таблице. Теперь в шаблоне необходимо создать UNI. Вы можете удалить шаблон UNI, нажав сначала на него, затем на кнопку **Удалить** в блоке **Действия** вверху справа.
4. Нажмите на созданный шаблон UNI и выберите вкладку **UNI**.
5. Нажмите на кнопку **+ Добавить шаблон UNI**.
6. В открывшемся окне настройте параметры UNI, выполнив следующие действия:
   - В поле **Имя** введите имя UNI.
   - В поле **OpenFlow-интерфейс** введите номер OpenFlow-интерфейса, поверх которого требуется создать UNI.
   - В раскрывающемся списке **Тип сегментации** выберите тип инкапсуляции на UNI:
     - **Access** – это значение выбрано по умолчанию.
     - **VLAN** – при выборе этого значения вам нужно ввести внешнюю метку VLAN в поле **VLAN ID**. Диапазон значений: от 1 до 4094.
     - **Q-in-Q** – при выборе этого значения вам нужно ввести внешнюю метку VLAN в поле **VLAN ID** и внутреннюю метку VLAN в поле **Внутренний VLAN ID**. Диапазон значений: от 1 до 4094.
7. Нажмите на кнопку **Добавить**.

   UNI отобразится в таблице. Вы можете выполнить одно из следующих действий с UNI, нажав на соответствующую кнопку рядом с ним в столбце **Действия**:
   - Изменить параметры UNI, нажав на кнопку **Изменить**.
   - Удалить UNI, нажав на кнопку **Удалить**.
8. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона UNI.

Создание UNI

UNI на устройстве CPE создаются автоматически из шаблона. Шаблон UNI применяется к устройствам при их первичном создании или регистрации.

Вы можете создавать UNI на отдельных устройствах CPE. Перед выполнением этой инструкции требуется активировать устройство CPE.

Чтобы создать UNI на устройстве CPE:

1. В области настройки устройства CPE выберите вкладку **UNI**.

2. Нажмите на кнопку **+ Добавить UNI**.

3. В открывшемся окне настройте параметры UNI, выполнив следующие действия:

   - В поле **Имя** введите имя UNI.
   - В раскрывающемся списке **Порт** выберите OpenFlow-интерфейс, поверх которого требуется создать UNI.
   - В раскрывающемся списке **Тип сегментации** выберите тип инкапсуляции на UNI:
     - **Access** – это значение выбрано по умолчанию.
     - **VLAN** – при выборе этого значения вам нужно ввести внешнюю метку VLAN поле **VLAN ID**. Диапазон значений: от 1 до 4094.
     - **Q-in-Q** – при выборе вам нужно ввести внешнюю метку VLAN в поле **VLAN ID** и внутреннюю метку VLAN в поле **Внутренний VLAN ID**. Диапазон значений: от 1 до 4094.
   - В раскрывающемся списке **QoS** выберите правило качества обслуживания для UNI.

4. Нажмите на кнопку **Добавить**.

   UNI отобразится в таблице. Вы можете выполнить одно из следующих действий с UNI, нажав на соответствующую кнопку рядом с ним в столбце **Действия**:

   - Изменить параметры UNI, нажав на кнопку **Изменить**.
   - Удалить UNI, нажав на кнопку **Удалить**.

5. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства CPE.

Создание группы OpenFlow-интерфейсов

Вы можете объединять 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.

Чтобы создать группу OpenFlow-интерфейсов:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Группы OF-интерфейсов**.

2. Нажмите на кнопку **+ Добавить группу OF-интерфейсов**.

3. В открывшемся окне настройте параметры группы OpenFlow-интерфейсов, выполнив следующие действия:

   - В поле **Имя** введите имя группы OpenFlow-интерфейсов.

- В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и OpenFlow-интерфейс, который вы хотите добавить в группу.

4. Нажмите на кнопку **Создать**.

Группа OpenFlow-интерфейсов отобразится в таблице. Вы можете выполнить одно из следующих действий с группой OpenFlow-интерфейсов, нажать на кнопку **Управление** рядом с ней и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры группы OpenFlow-интерфейсов, выбрав **Изменить**.
- Удалить группу OpenFlow-интерфейсов, выбрав **Удалить**.

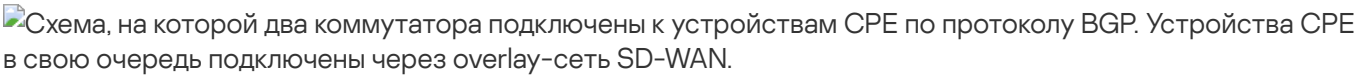
Протокол динамической маршрутизации BGP

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).

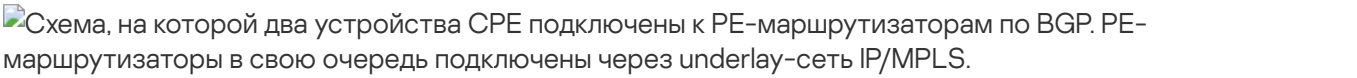
Также поддерживается установка динамических TCP-сессий с группами BGP-соседей (англ. BGP peer groups). Установив динамическую TCP-сессию, вам не нужно создавать отдельных BGP-соседей (англ. BGP peers).

На рисунках ниже представлены примеры использования протокола динамической маршрутизации BGP в решении:

- Подключение нескольких клиентских площадок к сети L3 SD-WAN по BGP.

  
  Схема, на которой два коммутатора подключены к устройствам CPE по протоколу BGP. Устройства CPE в свою очередь подключены через overlay-сеть SD-WAN.

- Подключение устройств CPE к операторской сети IP/MPLS по BGP.

  
  Схема, на которой два устройства CPE подключены к PE-маршрутизаторам по BGP. PE-маршрутизаторы в свою очередь подключены через underlay-сеть IP/MPLS.

- Использование BGP для настройки связности устройств CPE внутри домена Kaspersky SD-WAN

  
  Схема, на которой настроена связность устройств CPE с помощью BGP через шлюз SD-WAN поверх наложенной сети SD-WAN.

Настройка протокола BGP

Вы можете настроить параметры использования протокола динамической маршрутизации BGP в шаблоне CPE или на отдельном устройстве.

Чтобы настроить протокол BGP:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры BGP**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. В раскрывающемся списке **BGP** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

4. Настройте параметры BGP, выполнив следующие действия:

   - В поле **AS** введите номер вашей автономной системы. Диапазон значений: от 1 до 4 294 967 295.
   - В поле **ID устройства CPE** введите ID устройства CPE.
   - В поле **Лимит маршрутов** введите максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 8.
   - Установите флажок **Всегда сравнивать MED**, чтобы устройство CPE сравнивало атрибут MED (multi-exit discriminator) маршрутов, анонсированных из разных автономных систем. По умолчанию флажок снят.

     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 устройство CPE оставалось в таблицах маршрутизации BGP-соседей при перезагрузке. Таким образом, после перезагрузки устройство может продолжать участвовать в обмене маршрутной информацией. По умолчанию флажок снят.
   - Установите флажок **IPv4 unicast-маршруты по умолчанию**, чтобы устройство CPE по умолчанию обменивалось IPv4-маршрутами с BGP-соседями. По умолчанию флажок снят.
   - Установите флажок **BGP-таймеры**, чтобы настроить BGP-таймеры. Если вы установили этот флажок, настройте таймеры, выполнив следующие действия:

     - В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений BGP-соседям. Диапазон значений: от 0 до 65535.
     - 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 65535.

     По умолчанию флажок снят.

   - В блоке **Перераспределение маршрутов** установите флажки рядом с типами маршрутов, которые устройство CPE может анонсировать BGP-соседям. Если вы установили флажок рядом с типом маршрутов, укажите параметры маршрутизации, выполнив следующие действия:

     - В раскрывающемся списке **Карта маршрутизации** выберите карту маршрутизации для маршрутов.
     - В поле **Метрика** введите метрику маршрутов. Диапазон значений: от 0 до 4 294 967 295.

   - В блоке **Сети** нажмите на кнопку **+ Сеть** и укажите сеть, которую устройство CPE должно анонсировать BGP-соседям, выполнив следующие действия:

- В поле **Сеть** введите IP-адрес и маску подсети.
- В раскрывающемся списке **Карта маршрутизации** выберите карту маршрутизации для маршрутов.

Вы можете указать несколько сетей.

5. При необходимости выполните следующие действия:
   - Создайте списки управления доступом.
   - Создайте списки префиксов.
   - Создайте карты маршрутизации.
6. Создайте BGP-соседей и/или группы BGP-соседей.
7. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание списка управления доступом (ACL)

Список управления доступом (англ. Access Control List, ACL) – это набор правил, которые используются для 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.

Если ни одно из правил в списке управления доступом не может быть применено к маршруту, он будет отброшен.

Вы можете создавать списки управления доступом в шаблоне CPE или на отдельном устройстве.

Чтобы создать список управления доступом:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры BGP** → **Списки управления доступом**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.
3. Нажмите на кнопку **+ Добавить список управления доступом**.
4. В открывшемся окне укажите имя списка управления доступом. Максимальная длина: 50 символов.
5. Нажмите на кнопку **+ Добавить правило**.
6. Настройте параметры правила, выполнив следующие действия:

- В поле **Порядковый номер** укажите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.
- В раскрывающемся списке **Сеть** выберите тип правила:
  - **any** – правило, разрешающее или запрещающее анонсирование любых сетей.
  - **IP/MASK** – правило, разрешающее или запрещающее анонсирование определенной сети. Если вы выбрали это значение, введите IP-адрес и префикс сети в поле справа. Это значение выбрано по умолчанию.
- В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:
  - **Permit** – разрешать анонсирование маршрутов. Это значение выбрано по умолчанию.
  - **Deny** – запрещать анонсирование маршрутов.

7. Нажмите на кнопку **Сохранить**.

   Список управления доступом отобразится в таблице. Вы можете выполнить одно из следующих действий со списком управления доступом, нажав на соответствующую кнопку рядом с ним в столбце **Управление**:

   - Изменить параметры списка управления доступом, нажав на кнопку **Изменить**.
   - Удалить список управления доступом, нажав на кнопку **Удалить**.

8. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание списка префиксов (prefix list)

Список префиксов (англ. prefix list) 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.

Если ни одно из правил в списке префиксов не может быть применено к маршруту, он будет отброшен.

Вы можете создавать списки префиксов в шаблоне CPE или на отдельном устройстве.

Чтобы создать список префиксов:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры BGP** → **Списки префиксов**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Нажмите на кнопку **+ Добавить список префиксов**.
4. В открывшемся окне укажите имя списка префиксов. Максимальная длина: 50 символов.

5. Нажмите на кнопку **+ Добавить правило**.

6. Настройте параметры правила, выполнив следующие действия:

   - В поле **Порядковый номер** введите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.

   - В раскрывающемся списке **Сеть** выберите тип правила:

     - **any** – правило, разрешающее или запрещающее анонсирование любых сетей.

     - **IP/MASK** – правило, разрешающее или запрещающее анонсирование определенной сети. Если вы выбрали это значение, введите IP-адрес и префикс сети в поле справа. Это значение выбрано по умолчанию.

   - В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:

     - **Permit** – разрешать анонсирование маршрутов. Это значение выбрано по умолчанию.

     - **Deny** – запрещать анонсирование маршрутов.

   - В полях **Greater or Equal** и **Less or Equal** укажите диапазон префиксов. Диапазон значений от 0 до 32.

7. Нажмите на кнопку **Сохранить**.

   Список префиксов отобразится в таблице. Вы можете выполнить одно из следующих действий со списком префиксов, нажав на соответствующую кнопку рядом с ним в столбце **Управление**:

   - Изменить параметры списка префиксов, нажав на кнопку **Изменить**.

   - Удалить список префиксов, нажав на кнопку **Удалить**.

8. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание карты маршрутизации (route map)

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 карте маршрутизации не может быть применено к маршруту, он будет отброшен.

Вы можете создавать карты маршрутизации в шаблоне CPE или на отдельном устройстве.

Чтобы создать карту маршрутизации:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры BGP** → **Карты маршрутизации**.

2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Нажмите на кнопку **+ Добавить карту маршрутизации**.

4. В открывшемся окне укажите имя карты маршрутизации. Максимальная длина: 50 символов.

5. Нажмите на кнопку **+ Добавить правило**.

6. Настройте параметры правила, выполнив следующие действия:

   - В поле **Порядковый номер** введите порядковый номер правила. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.

   - В раскрывающемся списке **Действие** выберите действие, которое правило должно применять к маршрутам:

     - **Permit** – разрешать анонсирование маршрутов. Это значение выбрано по умолчанию.

     - **Deny** – запрещать анонсирование маршрутов.

   - В раскрывающемся списке **Условие** выберите условие, выполнение которого необходимо для применения правила к маршруту:

     - **None** – 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 списку префиксов, который вам нужно выбрать в раскрывающемся списке **or (depends on type)**.

     - **Community** – применять правило к маршрутам, имеющим атрибут community со значением, которое вам нужно ввести в поле **Значение**.

     - **Extcommunity** – применять правило к маршрутам, имеющим атрибут extended community со значением, которое вам нужно ввести в поле **Значение**.

   - В раскрывающемся списке **Изменять атрибут** выберите атрибут, значение которого требуется изменять при применении правила к маршруту:

     - **None** – не изменять значения атрибутов. Это значение выбрано по умолчанию.

     - **IP next-hop** – изменять значение атрибута next hop. В качестве нового значения требуется ввести IP-адрес.

     - **Local Preference** – изменять значение атрибута local preference. Диапазон значений: от 0 до 4 294 967 295.

     - **Metric** – изменять значение атрибута MED. Диапазон значений: от 0 до 4 294 967 295.

     - **Community** – изменять значение атрибута community.

     - **Extcommunity** – изменять значение атрибута extended community.

- **VPNv4 next-hop** – изменять значение атрибута next hop для VPNv4-маршрутов. В качестве нового значения требуется ввести IPv4-адрес.

- **AS Path Preprend** – добавлять номер автономной системы в атрибут as path. Вы можете указать несколько номеров через пробел.

- В поле **Новое значение** введите значение, которое требуется присвоить атрибуту. В зависимости от атрибута, выбранного в раскрывающемся списке **Изменять атрибут**, вы можете вводить цифры или символы.

7. Нажмите на кнопку **Сохранить**.

   Карта маршрутизации отобразится в таблице. Вы можете выполнить одно из следующих действий с картой маршрутизации, нажав на соответствующую кнопку рядом с ней в столбце **Управление**:

   - Изменить параметры карты маршрутизации, нажав на кнопку **Изменить**.

   - Удалить карту маршрутизации, нажав на кнопку **Удалить**.

8. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание BGP-соседа (BGP peer)

Вы можете создавать BGP-соседей в шаблоне CPE или на отдельном устройстве. Максимальное количество динамических BGP-соседей: 512.

Чтобы создать BGP-соседа:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры BGP** → **BGP-соседи**.

2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Нажмите на кнопку **+ Добавить BGP-соседа**.

4. В открывшемся окне настройте параметры BGP-соседа, выполнив следующие действия:

   - В поле **Имя** введите имя BGP-соседа. Максимальная длина: 50 символов.

   - Установите флажок **Выключить BGP-соседа**, чтобы не устанавливать TCP-сессию при создании BGP-соседа. По умолчанию флажок снят.

   - В поле **Адрес соседа** введите IP-адрес BGP-соседа.

   - В поле **AS** введите номер автономной системы BGP-соседа. Диапазон значений: от 1 до 4 294 967 295.

   - В поле **Описание** введите краткое описание BGP-соседа.

   - В поле **Пароль** 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.

- В поле **Loopback-интерфейс** введите IP-адрес loopback-интерфейса, который устройство CPE должно передавать BGP-соседу при установлении TCP-сессии.
- 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.
- Установите флажок **Уникальные BGP-таймеры**, чтобы настроить BGP-таймеры. Если вы установили этот флажок, настройте таймеры, выполнив следующие действия:
  - В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений BGP-соседям. Диапазон значений: от 0 до 65535.
  - 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 65535.

  По умолчанию флажок снят.
- Установите флажок **Включить BFD**, чтобы использовать протокол BFD для обнаружения сбоев в TCP-сессии. По умолчанию флажок снят.

  Одновременное использование протокола BFD и функции Graceful Restart может привести к сбоям в работе TCP-сессии между BGP-соседями.

5. Если вы хотите указать дополнительные параметры BGP-соседа, выберите вкладку **Расширенные параметры** и выполните следующие действия:
   - 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. По умолчанию флажок снят.
   - 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. По умолчанию флажок снят.
   - Установите флажок **Неизменный атрибут Next Hop**, чтобы не изменять атрибут next hop маршрутов, которые устройство CPE анонсирует BGP-соседу. По умолчанию флажок снят.
   - Установите флажок **Собственный IP как Next Hop**, чтобы использовать IP-адрес устройства CPE в качестве атрибута next-hop при анонсировании маршрутов BGP-соседу. По умолчанию флажок снят.
   - Установите флажок **Неизменный атрибут MED**, чтобы не изменять атрибут MED маршрутов, которые устройство CPE анонсирует BGP-соседу. По умолчанию флажок снят.
   - 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 флажок снят.

- В поле **Дополнительная AS** введите номер дополнительной автономной системы, который устройство CPE должно передавать BGP-соседу. Диапазон значений: от 1 до 4 294 967 295.

- В поле **Вес** введите вес маршрутов, анонсируемых BGP-соседом. Чем больше вес маршрута, тем больше его приоритет. Диапазон значений: от 0 до 65535.

- В поле **Лимит префиксов** введите максимальное количество префиксов, которое BGP-сосед может анонсировать устройству CPE. Диапазон значений: от 1 до 4 294 967 295.

- Установите флажок **Отправлять community**, чтобы устройство CPE анонсировало BGP-соседу маршруты с атрибутом community. Если вы установили этот флажок, выберите тип отправляемого атрибута:

  - **All** – устройство может отправлять BGP-соседу все доступные типы атрибута community.

  - **Both** – устройство может отправлять BGP-соседу атрибуты standard community и extended community.

  - **Extended** – устройство может отправлять BGP-соседу атрибут extended community.

  - **Large** – устройство может отправлять BGP-соседу атрибут large community.

  - **Standard** – устройство может отправлять BGP-соседу атрибут standard community.

  По умолчанию флажок снят.

- Установите флажок **Отправлять 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**, чтобы выбрать карту маршрутизации для маршрута по умолчанию.

6. Если вы хотите настроить фильтрацию маршрутов для BGP-соседа, выберите вкладку **Фильтрация** и выполните следующие действия:

   - В блоке **Карта маршрутизации** выберите карты маршрутизации для фильтрации маршрутной информации, выполнив следующие действия:

     - В раскрывающемся списке **Входящие** выберите карту маршрутизации, которую BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.

     - В раскрывающемся списке **Исходящие** выберите карту маршрутизации, которую устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

   - В блоке **Список префиксов** выберите списки префиксов для фильтрации маршрутной информации, выполнив следующие действия:

     - В раскрывающемся списке **Входящие** выберите список префиксов, который BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.

     - В раскрывающемся списке **Исходящие** выберите список префиксов, который устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

   - В блоке **Список управления доступом** выберите списки управления доступом для фильтрации маршрутной информации, выполнив следующие действия:

- В раскрывающемся списке **Входящие** выберите список управления доступом, который BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.
- В раскрывающемся списке **Исходящие** выберите список управления доступом, который устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

7. Нажмите на кнопку **Сохранить**.

   BGP-сосед отобразится в таблице. Вы можете выполнить одно из следующих действий с BGP-соседом, нажав на соответствующую кнопку рядом с ним в столбце **Управление**:

   - Изменить параметры BGP-соседа, нажав на кнопку **Изменить**.
   - Удалить BGP-соседа, нажав на кнопку **Удалить**.

8. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание группы BGP-соседей (BGP peer group)

Вы можете создавать группы BGP-соседей в шаблоне CPE или на отдельном устройстве.

Чтобы создать группу BGP-соседей:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры BGP** → **Группы BGP-соседей**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Нажмите на кнопку **+ Добавить группу BGP-соседей**.
4. В открывшемся окне настройте параметры группы BGP-соседей, выполнив следующие действия:
   - В поле **Имя** введите имя группы BGP-соседей. Максимальная длина: 50 символов.
   - Установите флажок **Выключить группу BGP-соседей**, чтобы не устанавливать TCP-сессию при создании группы BGP-соседей. По умолчанию флажок снят.
   - В поле **BGP Listen Range** введите диапазон IP-адресов группы BGP-соседей, который определяется с помощью префикса.
   - В поле **AS** введите номер автономной системы группы BGP-соседей. Диапазон значений: от 1 до 4 294 967 295.
   - В поле **Описание** введите краткое описание группы BGP-соседей.
   - В поле **Пароль** 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.

- В поле **Loopback-интерфейс** введите IP-адрес loopback-интерфейса, который устройство CPE должно передавать группе BGP-соседей при установлении TCP-сессии.

- 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.

- Установите флажок **Уникальные BGP-таймеры**, чтобы настроить BGP-таймеры. Если вы установили этот флажок, настройте таймеры, выполнив следующие действия:

  - В поле **Keepalive** введите интервал времени в секундах для отправки устройством CPE keepalive-сообщений группе BGP-соседей. Диапазон значений: от 0 до 65535.

  - 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 65535.

  По умолчанию флажок снят.

- Установите флажок **Включить BFD**, чтобы использовать протокол BFD для обнаружения сбоев в TCP-сессии. По умолчанию флажок снят.

  Одновременное использование протокола BFD и функции Graceful Restart может привести к сбоям в работе TCP-сессии между BGP-соседями.

5. Если вы хотите указать дополнительные параметры группы BGP-соседей, выберите вкладку **Расширенные параметры** и выполните следующие действия:

   - Установите флажок **Soft-reconfiguration inbound**, чтобы хранить анонсированные группой BGP-соседей 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 группе BGP-соседей. По умолчанию флажок снят.

   - 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. По умолчанию флажок снят.

   - Установите флажок **Неизменный атрибут Next Hop**, чтобы не изменять атрибут next hop маршрутов, которые устройство CPE анонсирует группе BGP-соседей. По умолчанию флажок снят.

   - Установите флажок **Собственный IP как Next Hop**, чтобы использовать IP-адрес устройства CPE в качестве атрибута next-hop при анонсировании маршрутов группе BGP-соседей. По умолчанию флажок снят.

   - Установите флажок **Неизменный атрибут MED**, чтобы не изменять атрибут MED маршрутов, которые устройство CPE анонсирует группе BGP-соседей. По умолчанию флажок снят.

   - 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 флажок снят.

- В поле **Дополнительная AS** введите номер дополнительной автономной системы, который устройство CPE должно передавать группе BGP-соседей. Диапазон значений: от 1 до 4 294 967 295.

- В поле **Вес** введите вес маршрутов, анонсируемых группой BGP-соседей. Чем больше вес маршрута, тем больше его приоритет. Диапазон значений: от 0 до 65535.

- 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.

- Установите флажок **Отправлять community**, чтобы устройство CPE анонсировало группе BGP-соседей маршруты с атрибутом community. Если вы установили этот флажок, выберите тип отправляемого атрибута:

  - **All** – устройство может отправлять BGP-соседу все доступные типы атрибута community.

  - **Both** – устройство может отправлять BGP-соседу атрибуты standard community и extended community.

  - **Extended** – устройство может отправлять BGP-соседу атрибут extended community.

  - **Large** – устройство может отправлять BGP-соседу атрибут large community.

  - **Standard** – устройство может отправлять BGP-соседу атрибут standard community.

  По умолчанию флажок снят.

- Установите флажок **Отправлять 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**, чтобы выбрать карту маршрутизации для маршрута по умолчанию.

6. Если вы хотите настроить фильтрацию маршрутов для группы BGP-соседей, выберите вкладку **Фильтрация** и выполните следующие действия:

   - В блоке **Карта маршрутизации** выберите карты маршрутизации для фильтрации маршрутной информации, выполнив следующие действия:

     - В раскрывающемся списке **Входящие** выберите карту маршрутизации, которую группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.

     - В раскрывающемся списке **Исходящие** выберите карту маршрутизации, которую устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.

   - В блоке **Список префиксов** выберите списки префиксов для фильтрации маршрутной информации, выполнив следующие действия:

     - В раскрывающемся списке **Входящие** выберите список префиксов, который группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.

     - В раскрывающемся списке **Исходящие** выберите список префиксов, который устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.

   - В блоке **Список управления доступом** выберите списки управления доступом для фильтрации маршрутной информации, выполнив следующие действия:

     - В раскрывающемся списке **Входящие** выберите список управления доступом, который группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.

- В раскрывающемся списке **Исходящие** выберите список управления доступом, который устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.

7. Нажмите на кнопку **Сохранить**.

   Группа BGP-соседей отобразится в таблице. Вы можете выполнить одно из следующих действий с группой BGP-соседей, нажав на соответствующую кнопку рядом с ней в столбце **Управление**:

   - Изменить параметры группы BGP-соседей, нажав на кнопку **Изменить**.
   - Удалить группу BGP-соседей, нажав на кнопку **Удалить**.

8. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Настройка протокола 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**.

Контролирует передачу пакетов трафика по сети через устройства CPE. В плоскость управления трафиком входят оркестратор и контроллер SD-WAN.

Осуществляет передачу пакетов трафика. Плоскость передачи данных образуют устройства CPE.

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.

Вы можете настроить протокол BFD в шаблоне CPE или на отдельном устройстве.

Чтобы настроить протокол BFD:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Параметры BFD**.

2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. В раскрывающемся списке **BFD** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

   Если вы включили BFD, вам нужно создать BFD-соседа.

4. Нажмите на кнопку **+ Добавить BFD-соседа**.

5. В открывшемся окне настройте параметры BFD-соседа, выполнив следующие действия:

   - В поле **Имя** введите имя BFD-соседа. Максимальная длина: 255 символов.
   - В поле **IP-адрес** введите IP-адрес BFD-соседа.
   - В поле **Интервал передачи** введите интервал времени в миллисекундах для отправки контрольных пакетов BFD-соседу. Диапазон значений: от 60 до 10000.
   - В поле **Интервал получения** введите интервал времени в миллисекундах для получения контрольных пакетов от BFD-соседа. Диапазон значений от 60 до 10000.
   - 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.

6. Нажмите на кнопку **Сохранить**.

   BFD-сосед отобразится в таблице. Вы можете выполнить одно из следующих действий с BFD-соседом, нажав на соответствующую кнопку рядом с ним в столбце **Действия**:

   - Изменить параметры BFD-соседа, нажав на кнопку **Изменить**.
   - Удалить BFD-соседа, нажав на кнопку **Удалить**.

7. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание 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 создавать статические IPv4-маршруты в шаблоне CPE или на отдельном устройстве.

Чтобы создать статический IPv4-маршрут:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Статические маршруты**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Нажмите на кнопку создания статического IPv4-маршрута кнопка в виде знака плюс и настройте его параметры, выполнив следующие действия:

- В раскрывающемся списке **Интерфейс** выберите сетевой интерфейс для отправки пакетов трафика на узел назначения.
- В поле **Узел назначения** введите IP-адрес узла назначения.
- В поле **Маска подсети IPv4** введите маску подсети узла назначения.
- В поле **Шлюз** введите IP-адрес шлюза для маршрутизации трафика.
- В поле **Метрика** введите метрику маршрута. По умолчанию указано значение `0`.
- В поле **MTU** введите значение MTU для маршрута.
- 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.

Вы можете удалить статический IPv4-маршрут, нажав на кнопку удаления кнопка в виде знака минус рядом с ним.

4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства 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.

Создание экземпляра VRRP

Вы можете создавать экземпляры VRRP в шаблоне CPE или на отдельном устройстве.

Чтобы настроить протокол VRRP:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **VRRP**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.
3. В раскрывающемся списке **VRRP** выберите одно из следующих значений:

   - **Включено**.
   - **Выключено** – это значение выбрано по умолчанию.

   Для создания экземпляра требуется включить VRRP.
4. Нажмите на кнопку **+ Добавить экземпляр VRRP**.
5. В открывшемся окне настройте параметры экземпляра VRRP, выполнив следующие действия:

   - В поле **Имя** введите имя экземпляра VRRP. Максимальная длина: 16 символов.
   - 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.
   - В раскрывающемся списке **Интерфейс** выберите сетевой интерфейс, которому будет назначен виртуальный IP-адрес.
   - 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.
   - В раскрывающемся списке **Состояние** выберите роль устройства CPE:

     - **BACKUP** – резервный VRRP-маршрутизатор. Это значение выбрано по умолчанию.
     - **MASTER** – основной VRRP-маршрутизатор.

- 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`.

- В поле **Интервал оповещения** введите интервал времени в секундах для отправки VRRP-объявлений. Диапазон значений: от 1 до 60. По умолчанию указано значение `5`.

- Установите флажок **Оставлять резервным при восстановлении**, чтобы не изменять роль резервного VRRP-маршрутизатора, ставшего основным, даже если прежний основной VRRP-маршрутизатор восстанавливает работу. По умолчанию флажок снят.

- Установите флажок **Unicast-рассылка**, чтобы настроить отправку VRRP-объявлений в виде unicast-сообщений. По умолчанию флажок снят. Если вы установили флажок, настройте рассылку, выполнив следующие действия:

  - В поле **IP основного VRRP-маршрутизатора** введите требуемое значение.

  - В поле **IP резервного VRRP-маршрутизатора** введите требуемое значение.

- Установите флажок **Аутентификация**, чтобы указать пароль для аутентификации VRRP-объявлений. По умолчанию флажок снят. Если вы установили флажок, введите пароль в соответствующем поле. Максимальная длина: 16 символов. Вы можете просмотреть введенный пароль, нажав на кнопку просмотра .

6. Нажмите на кнопку **Сохранить**.

   Экземпляр VRRP отобразится в таблице. Вы можете выполнить одно из следующих действий с экземпляром VRRP, нажав на соответствующую кнопку рядом с ним в столбце **Действия**:

   - Изменить параметры экземпляра VRRP, нажав на кнопку **Изменить**.

   - Удалить экземпляр VRRP, нажав на кнопку **Удалить**.

7. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Создание группы экземпляров VRRP

Вы можете создавать группы экземпляров VRRP в шаблоне CPE или на отдельном устройстве. Перед выполнением этой инструкции требуется создать как минимум один экземпляр VRRP.

Чтобы создать группу экземпляров VRRP:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **VRRP → Группы экземпляров VRRP**.

2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Нажмите на кнопку **+ Группы экземпляров VRRP**.

4. В открывшемся окне настройте параметры группы экземпляров VRRP, выполнив следующие действия:

   - В поле **Имя** введите имя группы экземпляров VRRP. Максимальная длина: 16 символов. По умолчанию указано значение `1`.
   - В раскрывающемся списке **Экземпляры VRRP** выберите экземпляры, которые требуется добавить в группу.

5. Нажмите на кнопку **Сохранить**.

   Группа экземпляров VRRP отобразится в таблице. Вы можете выполнить одно из следующих действий с группой экземпляров VRRP, нажав на соответствующую кнопку рядом с ней в столбце **Действия**:

   - Изменить параметры группы экземпляров VRRP, нажав на кнопку **Изменить**.
   - Удалить группу экземпляров VRRP, нажав на кнопку **Удалить**.

6. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Настройка подключения пользователей к веб-консоли устройства CPE

Вы можете указать в шаблоне CPE параметры, которые будут использоваться для подключения пользователей к веб-консоли устройства.

Чтобы настроить подключение пользователей к веб-консоли устройства CPE:

1. В области настройки шаблона CPE выберите вкладку **Параметры веб-консоли**.
2. Настройте параметры подключения, выполнив следующие действия:

   - В раскрывающемся списке **Веб-консоль** выберите, могут ли пользователи подключаться к веб-консоли устройства CPE:
     - **Enable** – пользователи могут подключаться к веб-консоли.
     - **Disable** – пользователи не могут подключаться к веб-консоли. Это значение выбрано по умолчанию.
   - В поле **Порт** введите номер порта для подключения к веб-консоли. По умолчанию указано значение `80`.
   - В раскрывающемся списке **Протокол** выберите протокол для подключения к веб-консоли:
     - **http** – это значение выбрано по умолчанию.
     - **https**.

3. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

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 устройства к Syslog-серверу в шаблоне CPE или на отдельном устройстве.

Чтобы настроить подключение устройства CPE к Syslog-серверу:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Журналы**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.
3. Настройте параметры подключения, выполнив следующие действия:
   - 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.
   - В поле **IP или FQDN Syslog-сервера** введите требуемое значение.
   - В поле **Порт Syslog-сервера** введите требуемое значение. Диапазон значений: от 0 до 65353.
   - В раскрывающемся списке **Протокол Syslog-сервера** выберите протокол для передачи файлов журнала на Syslog-сервер:
     - **UDP** – это значение выбрано по умолчанию.
     - **TCP**.
   - В поле **Префикс для журналов** введите сообщение, которое требуется передавать с каждым файлом журнала на Syslog-сервер. Максимальная длина: 256 символов.
4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Настройка подключения устройства CPE к NTP-серверу

Вы можете настроить подключение к NTP-серверу в шаблоне CPE или на отдельном устройстве.

Чтобы настроить подключение устройства CPE к NTP-серверу:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **NTP**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.
3. Укажите параметры подключения:
   - Установите флажок **Подключиться к NTP-серверу**, чтобы разрешить устройству CPE подключаться к NTP-серверу. По умолчанию флажок установлен.

- В блоке **NTP-серверы** укажите IP-адрес или FQDN NTP-сервера и нажмите на кнопку **+ Добавить**. Пример значения: `server 0.pool.ntp.org`. Вы можете указать несколько серверов.

- Установите флажок **Использовать как NTP-сервер**, чтобы использовать устройство CPE в качестве NTP-сервера. По умолчанию флажок снят.

4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Просмотр ошибок

Система мониторинга присылает вам уведомления об ошибках, которые возникают во время работы устройства CPE. С помощью этих уведомлений вы можете определять и устранять причины неправильной работы устройств.

При возникновении ошибки ей присваивается один из следующих уровней критичности:

- Предупреждение.
- Средний.
- Высокий.
- Авария.

Параметры мониторинга, которые вы настраиваете 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.

Чтобы просмотреть ошибки на устройстве CPE,

в разделе настройки устройства CPE выберите вкладку **Проблемы**.

Отобразятся ошибки, возникшие при мониторинге устройства 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 этом устройстве.

Чтобы просмотреть параметры подключения к сети оператора связи на устройстве CPE,

в разделе настройки устройства CPE выберите вкладку **Модемы**.

Отобразятся все модемы, через которые устройство CPE подключено к сетям операторов связи, а также параметры этих подключений.

Добавление VIM в шаблон uCPE

Если при создании шаблона CPE вы выбрали тип **uCPE**, вы можете добавить в него **VIM** для управления **VNF**.

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

Менеджер, обеспечивающий управление и мониторинг вычислительных и сетевых ресурсов, а также ресурсов хранения в виртуальной инфраструктуре. С его помощью VNF взаимодействуют со всеми этими ресурсами.

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.

Чтобы добавить VIM в шаблон uCPE:

1. В области настройки шаблона CPE выберите вкладку **VIM**.
2. В открывшемся окне настройте параметры VIM, выполнив следующие действия:
   - В поле **Порт** введите номер порта для подключения оркестратора к VIM. По умолчанию указано значение `5000`.
   - В раскрывающемся списке **Протокол** выберите протокол для подключения оркестратора к VIM:
     - **http** – это значение выбрано по умолчанию.
     - **https**.
   - В поле **Имя пользователя** введите имя пользователя учетной записи OpenStack с правами администратора для авторизации в VIM.
   - В поле **Пароль** введите пароль учетной записи OpenStack с правами администратора для авторизации в VIM.
   - В поле **Проект администратора** введите имя проекта администратора OpenStack для авторизации в VIM.
   - В поле **Домен** введите имя OpenStack-домена.
   - В поле **Физическая VLAN-сеть** введите имя physnet для VLAN-сетей.
   - В раскрывающемся списке **За NAT** выберите, находится ли VIM за NAT (Network Address Translation):
     - **Включено** – VIM находится за NAT.
     - **Выключено** – VIM не находится за NAT. Это значение выбрано по умолчанию.

- В поле **Переподписка ЦП** введите коэффициент переподписки при предоставлении виртуальных процессорных ядер. По умолчанию указано значение `10`.
- В поле **Переподписка диска** введите коэффициент переподписки дискового пространства. По умолчанию указано значение `10`.
- В поле **Переподписка ОЗУ** введите коэффициент переподписки оперативной памяти. По умолчанию указано значение `10`.
- В поле **Диапазон VLAN ID** введите максимальное количество VLAN для OpenStack. Диапазон значений: от 0 до 4094. По умолчанию указано значение `4000`.

3. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Работа с прошивками

Kaspersky SD-WAN поддерживает обновление прошивок (англ. firmware) на устройствах CPE. Перед установкой новой версии прошивки ее необходимо добавить 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 добавлении архива с прошивкой.

Если версия прошивки на устройстве CPE устарела по сравнению с одной из добавленных прошивок, ее имя подсвечивается оранжевым цветом в столбце **Версия ПО** подраздела **Устройства CPE**. Для поиска устройств с устаревшей версией прошивки также можно использовать фильтр **Необходимо обновление**.

Вы можете устанавливать прошивки на устройствах CPE следующим образом:

- В подразделе **Устройства CPE** – вам нужно установить флажки рядом с одним или несколькими устройствами, после чего создать отложенную задачу по обновлению с помощью раскрывающегося списка **Действия**.
- В разделе **Планировщик** – вам нужно заранее сгруппировать устройства, на которых вы хотите обновить прошивку, с помощью тегов, после чего создать отложенную задачу по обновлению.

При создании задачи по обновлению вы можете 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.

Задействованную в задаче по обновлению прошивку невозможно удалить.

> В процессе обновления прошивки устройство CPE перезагружается.

Добавление прошивки

Чтобы добавить прошивку:

1. В навигационной панели перейдите в раздел **SD-WAN**.
2. Нажмите на кнопку **+ Прошивка**.
3. Укажите путь к архиву с прошивкой. При указании пути вы можете выбрать несколько архивов одновременно.

Откроется подраздел **Прошивка**, и прошивка отобразится в таблице. Отображаемые параметры прошивки, например дата ее выпуска и совместимая модель устройства CPE, экспортируются из файла с метаданными.

Вы можете удалить прошивку, установив рядом с ней флажок и выбрав **Удалить** в раскрывающемся списке **Действия** вверху справа.

Поиск устройств CPE с устаревшей прошивкой

Чтобы найти устройства CPE с устаревшей прошивкой:

1. В навигационной панели перейдите в раздел **SD-WAN**.
2. Выполните одно из следующих действий:
   - Найдите устройства CPE с устаревшей прошивкой в столбце **Версия ПО**. Имена устаревших версий подсвечиваются оранжевым цветом.
   - Отобразите список устройств CPE с устаревшей прошивкой, нажав на кнопку **Необходимо обновление** в верхней части страницы.

Обновление прошивки

Вы можете обновлять прошивки на устройствах CPE в разделе **Планировщик** и подразделе **Устройства CPE** веб-интерфейса оркестратора. Перед выполнением этой инструкции требуется выполнить следующие действия:

- добавить прошивку;
- сгруппировать устройства CPE с помощью тегов, если вы планируете обновлять прошивку в разделе **Планировщик**.

Чтобы обновить прошивку на устройстве CPE:

1. Откройте окно установки прошивки, выполнив одно из следующих действий:
   - В навигационной панели перейдите в раздел **Планировщик** и нажмите на кнопку **+ Отложенная задача**.
   - В навигационной панели перейдите в раздел **SD-WAN**, установите флажки рядом с устройствами CPE, на которых требуется обновить прошивку, и в раскрывающемся списке **Действия** вверху справа выберите **Обновить прошивку**.
2. В открывшемся окне настройте параметры прошивки, выполнив следующие действия:

- Если вы обновляете прошивку в разделе **Планировщик**, в раскрывающемся списке **Тип** выберите **Обновление прошивки CPE**.

- В поле **Имя** введите имя отложенной задачи.

- В раскрывающемся списке **Версия** выберите прошивку, которую требуется установить на устройстве CPE.

- В поле **Дата и время выполнения** введите дату и время для выполнения отложенной задачи. По умолчанию указана дата и время в момент, когда вы начали создавать отложенную задачу.

- Установите флажок **Сохранить конфигурацию CPE**, чтобы сохранить конфигурацию устройства CPE после обновления прошивки. Если флажок снят, после установки прошивки параметры устройства сбрасываются до заводских значений. По умолчанию флажок установлен.

- Установите флажок **Принудительное обновление**, чтобы установить прошивку принудительно, даже если внутренняя проверка на устройстве CPE выявляет несовместимость его текущей прошивки с новой. По умолчанию флажок снят.

- Если вы обновляете прошивку в разделе **Планировщик**, в поле **Теги** введите теги устройств CPE, на которых требуется обновить прошивку.

3. 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.

4. Выполните одно из следующих действий:

   - Если вы обновляете прошивку в разделе **Планировщик**, нажмите на кнопку **Добавить**.

   - Если вы обновляете прошивку в подразделе **Устройства CPE**, нажмите на кнопку **Запланировать**.

Отложенная задача по обновлению отобразится в подразделе **Обновление прошивки CPE** раздела **Планировщик**. Обновление прошивки на устройстве CPE начнется в указанное вами время.

Вы можете выполнить одно из следующих действий с отложенной задачей, нажав сначала на нее, затем на соответствующую кнопку в блоке **Действия**:

- Выполнить отложенную задачу вручную, нажав на кнопку **Выполнить сейчас**.

- Удалить отложенную задачу, нажав на кнопку **Удалить**.

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.

Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Заранее развернутая сетевая функция, которая в готовом виде загружается в веб-интерфейс оркестратора. Оркестратор может осуществлять дальнейшую конфигурацию PNF.

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

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 для автоматического создания, обновления и удаления соответствующих им хостов 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.

Обратите внимание, что мониторинг VNF необходим для использования функций обеспечения доступности (англ. auto healing) и автоматического добавления или освобождения ресурсов (англ. auto scaling). 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.

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 вам нужно развернуть его в одном из ваших центров обработки данных.

Чтобы подключиться к серверу Zabbix:

1. В навигационной панели перейдите в раздел **Мониторинг**.
2. Настройте параметры подключения к серверу Zabbix, выполнив следующие действия:
   - В поле **URL** введите URL-адрес Zabbix API. Оркестратор отправляет по этому адресу HTTP-запросы для получения и отображения результатов мониторинга в виде графиков.

     Адрес состоит из URL 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`.
   - 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 авторизации на сервере Zabbix при отправке API-запроса.
   - В поле **Пароль** введите пароль пользователя для подключения к Zabbix API.
   - 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.
   - В поле **Группа для устройств 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.
   - В поле **Интервал для уведомлений** 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`.
3. 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 .
4. При необходимости нажмите на кнопку **Проверить соединение**, чтобы проверить доступность сервера Zabbix.
5. Нажмите на кнопку **Применить**.

Подключение к серверу Zabbix-прокси

Интеграция с Zabbix обеспечивает мониторинг компонентов решения. Перед подключением к серверу Zabbix-прокси вам нужно развернуть его в одном из ваших центров обработки данных.

Чтобы подключиться к серверу Zabbix-прокси:

1. На странице управления инфраструктурой решения в панели **Ресурсы** выберите вкладку **ЦОД**.
2. Нажмите на центр обработки данных, в котором развернут сервер Zabbix-прокси.
3. Выберите вкладку **Системные ресурсы**.
4. В блоке **Zabbix-прокси** настройте параметры Zabbix-прокси, выполнив следующие действия:
   - В поле **Имя** введите имя сервера Zabbix-прокси. Введенное имя должно совпадать с именем, указанным в параметрах сервера Zabbix-прокси.
   - В поле **IP** введите IP-адрес сервера Zabbix-прокси.
5. Нажмите на кнопку **Применить**.

Настройка мониторинга в шаблоне CPE

Вам нужно настроить мониторинг в шаблоне CPE и применить его к устройствам, на которых вы хотите просматривать результаты мониторинга.

Чтобы настроить мониторинг в шаблоне CPE:

1. В области настройки шаблона CPE выберите вкладку **Мониторинг**.
2. Настройте параметры мониторинга устройства CPE, выполнив следующие действия:
   - 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.
3. В поле **Шаблон Zabbix** введите имя шаблона Zabbix.
4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Просмотр результатов мониторинга

Вы можете просматривать результаты в следующих подразделах веб-интерфейса оркестратора:

- **Устройства CPE** – для просмотра результатов мониторинга отдельного устройства. Если вы планируете просматривать результаты мониторинга отдельного устройства, перед выполнением этой инструкции требуется настроить параметры мониторинга в примененном к нему шаблоне CPE.
- **Экземпляры SD-WAN** – для просмотра результатов мониторинга экземпляра SD-WAN.

Чтобы просмотреть результаты мониторинга:

1. В разделе настройки устройства CPE или экземпляра SD-WAN выберите вкладку **Мониторинг**.

2. По умолчанию отображаются результаты мониторинга за весь период. Вы можете отобразить результаты за требуемый период с помощью фильтра в верхней части страницы. Например, вы можете отобразить результаты за за год, за месяц или за произвольно заданный временной интервал.

3. Выберите параметр, для которого вы хотите отобразить результаты мониторинга.

Доступные результаты мониторинга отобразятся в виде графика.

Включение мониторинга на туннеле

Вы можете включать и выключать мониторинг на туннелях в разделах **Топология** и **Туннели**, а также в подразделе **Устройства CPE** веб-интерфейса оркестратора.

Чтобы включить мониторинг на туннеле:

1. Откройте окно мониторинга туннеля одним из следующих способов:

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Топология**, нажмите на туннель, на котором требуется включить мониторинг, и в открывшемся окне нажмите на кнопку **Пороговые значения мониторинга**.

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, на котором требуется включить мониторинг, и в раскрывающемся списке выберите **Пороговые значения мониторинга**.

   - В области настройки устройства CPE выберите вкладку **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, на котором требуется включить мониторинг, и в раскрывающемся списке выберите **Пороговые значения мониторинга**.

2. В открывшемся окне установите флажок **Включить мониторинг пороговых значений туннеля** и настройте параметры мониторинга, выполнив следующие действия:

   - Нажмите на кнопку **Установки по умолчанию**, чтобы использовать пороговые значения мониторинга по умолчанию.

   - Установите флажок **Нежелательный**, чтобы отметить туннель как нежелательный. *Нежелательные туннели* не используются при маршрутизации или используются в последнюю очередь, независимо от качества связи. По умолчанию флажок снят.

   - В поле **Интервал обработки ошибок туннеля и статистики 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`.

   - Установите флажок **Включить мониторинг ошибок туннеля**, чтобы указать пороговое значение количества ошибок на туннеле и в поле **Уровень критических ошибок туннеля, ошибок/сек** введите требуемое значение. Диапазон значений: от 1 до 1 000 000. По умолчанию флажок снят, а в поле указано значение `1000`.

   - Установите флажок **Включить мониторинг использования туннеля**, 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`.

   - В поле **Качество связи (задержка, джиттер, потеря пакетов), интервал обработки статистики** 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`.

- Установите флажок **Включить мониторинг задержек туннеля**, чтобы указать максимальное время задержки в миллисекундах при передаче пакетов по туннелю и в поле **Критический уровень задержек туннеля, мс** введите требуемое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, а в поле указано значение `100`.

- Установите флажок **Включить мониторинг джиттера туннеля**, чтобы указать максимальное время джиттера в миллисекундах при передаче пакетов по туннелю и в поле **Критический уровень джиттера туннеля, мс** введите требуемое значение. Диапазон значений: от 5 до 1000. По умолчанию флажок снят, а в поле указано значение `100`.

- Установите флажок **Включить мониторинг потерь пакетов туннеля**, чтобы указать максимальный процент потери пакетов на туннеле и в поле **Критический уровень потерь пакетов туннеля, %** введите требуемое значение. Диапазон значений: от 1 до 100. По умолчанию флажок снят, а в поле указано значение `2`.

3. Выполните одно из следующих действий:

   - 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.

4. Если вы включили функцию мониторинга на туннеле в подразделе **Устройства CPE**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства.

Просмотр состояния компонентов решения

Вы можете просматривать информацию о состоянии компонентов решения в разделе **Обозреватель**, который открывается автоматически после того, как вы авторизуетесь в веб-интерфейсе оркестратора.

Чтобы просмотреть состояние компонентов решения,

в навигационной панели перейдите в раздел **Обозреватель**.

Информация о каждом из компонентов решения распределена между отдельными блоками. Например, в блоке **Недоступные устройства CPE** отображаются устройства CPE, доступ к которым был потерян. Если компонент решения работает правильно, в блоке, соответствующем этому компоненту, отображается сообщение *Все работает правильно*.

Блоки можно перетаскивать мышью для изменения порядка их отображения. Вверху справа у каждого блока есть кнопка обновления , при нажатии на которую сбрасывается вся отображаемая информация. Вы также можете использовать кнопку настройки в правом верхнем углу страницы для сброса статистики и изменения интервала обновления информации в блоках.

Построение топологии

Соединение между устройствами CPE устанавливается через туннели, которые строятся поверх каналов передачи данных. Туннели являются однонаправленными, поэтому при установке соединения между двумя устройствами или между устройством и плоскостью управления сетью требуется построить как входящий, так и исходящий туннель.

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, являются *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 создавать и удалять, а также изменять их параметры.

  Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

- **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** – втоматически 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.

Туннели образуют топологию, которая определяет связность между устройствами CPE в **плоскости передачи данных** и отвечает за оптимальность прохождения трафика транспортных сервисов между устройствами.

Осуществляет передачу пакетов трафика. Плоскость передачи данных образуют устройства CPE.

Топология Hub-and-Spoke

Топология Hub-and-Spoke – это сетевая архитектура, в рамках которой центральная площадка (англ. hub) подключается к нескольким удаленным площадкам (англ. spokes) 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, в которой производится его анализ и фильтрация. Использование топологии Hub-and-Spoke также позволяет более эффективно использовать полосу пропускания за счет оптимизации и приоритизации трафика на центральной площадке.

В подразделах ниже 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.


На схеме изображены две площадки, соединенные с центральным офисом.

Для построения такой топологии вам нужно создать транспортный сервис P2M. В качестве точек назначения требуется использовать сервисные интерфейсы на шлюзах SD-WAN 1 и 2 и назначить им роль Root.

Устройства CPE, регистрирующиеся в оркестраторе, автоматически включаются в транспортный сервис с ролью Leaf и могут находиться за NAT (Network Address Translation) и PAT (Port Address Translation). В рамках этой топологии запрещается передача трафика напрямую между устройствами CPE.

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.


На схеме изображены две площадки, соединенные с центральным офисом и между собой.

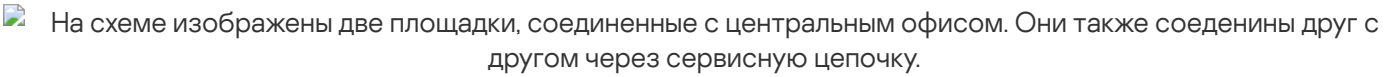
Для построения такой топологии вам нужно создать транспортный сервис P2M или M2M. В качестве точек назначения требуется использовать сервисные интерфейсы на шлюзах SD-WAN 1 и 2. При использовании транспортного сервиса P2M сервисным интерфейсам требуется назначить роль Root.

Устройства CPE, регистрирующиеся в оркестраторе, автоматически включаются в транспортный сервис и могут находиться за NAT и PAT.

Hub-and-Spoke со связью между удаленными офисами через сервисную цепочку в ЦОД

На рисунке ниже представлена топология, в рамках которой трафик между удаленными площадками проходит через **VNF**, развернутые в ЦОД. Сети SD-WAN, построенные с применением этой топологии, предоставляют возможность выполнения большого количества дополнительных задач, например обеспечения безопасности межсетевого обмена, наблюдения за пакетами трафика и кеширования данных.

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


На схеме изображены две площадки, соединенные с центральным офисом. Они также соеденины друг с другом через сервисную цепочку.

Для построения такой топологии вам нужно создать транспортный сервис P2M. Затем нужно убедиться, что сетевой сервис SD-WAN, развернутый для тенанта, содержит в цепочке все требуемые VNF.

Топологии 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.

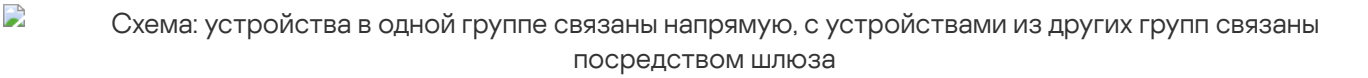
Построение прямых туннелей между устройствами CPE улучшает производительность Kaspersky SD-WAN благодаря следующим свойствам:

- 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 шлюз.



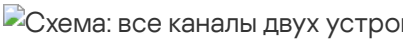
Топология Partial-Mesh

Устройство CPE может входить одновременно в несколько групп, как показано на рисунке ниже.

Топология Partial-Mesh, устройства CPE входят в несколько групп

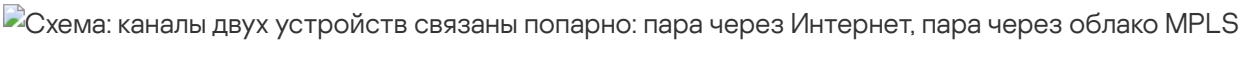
При построении P2P-туннелей, в зависимости от связности устройств CPE через физические каналы передачи данных, возможны следующие варианты наложенной связности:

- 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 из-за наличия NAT/PAT или ACL в интернете из-за топологии MPLS, не поддерживающей прямую связь между устройствами.

Вы можете добавить устройство в сеть определенной топологией с помощью топологических тегов.

Назначение топологических тегов устройству CPE

Топологические теги используются для построения топологий Full-Mesh и Partial-Mesh. Вы можете назначать топологические теги устройству CPE в подразделах **Устройства CPE** и **Шаблоны CPE** веб-интерфейса оркестратора.

Одновременно с топологическими тегами устройству CPE назначается роль – стандартное устройство или шлюз SD-WAN. Стандартные устройства автоматически устанавливают туннели с шлюзами SD-WAN, которые в свою очередь устанавливают туннели со всеми устройствами в сети, включая другие шлюзы.

Устройство CPE может быть транзитным. В этом случае другие устройства могут устанавливать через него туннели.

Возможны следующие варианты топологий:

- Hub-and-Spoke – топология по умолчанию, которая используется, если устройствам CPE не назначено топологических тегов. Вам нужно установить соединения между устройствами через центральный шлюз SD-WAN. В этом случае между устройствами не устанавливаются прямые туннели.
- Full-Mesh – вам нужно назначить устройствам CPE одинаковый топологический тег для реализации этой топологии. Все устройства с одинаковым топологическим тегом устанавливают прямые туннели между собой.
- Partial-Mesh – вам нужно сгруппировать устройства CPE путем назначения одного топологического тега одной группе устройств и другого топологического тега другой группе. В этом случае все устройства CPE из одной группы (с одинаковым топологическим тегом) устанавливают прямые туннели между собой, а с устройствами из другой группы связываются через шлюз. При назначении устройству CPE топологических тегов двух групп вы определяете его одновременно в обе группы. В этом случае устройство пытается установить прямые туннели к устройствам в обеих группах.

Топологические теги отличаются от обычных тегов тем, что обычные теги предназначены для классификации устройств CPE по произвольным признакам, в то время как топологические теги нужны для объединения устройств в сети с указанной топологией.

Чтобы назначить топологический тег устройству CPE:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Топология**.
2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. Настройте параметры, определяющие принадлежность устройства CPE к топологии, выполнив следующие действия:

   - В раскрывающемся списке **Роль** выберите роль устройства CPE в топологии:

     - **CPE** – стандартное устройство для реализации любой топологии. Это значение выбрано по умолчанию.

     - **Шлюз** – шлюз SD-WAN для реализации топологии Hub-and-Spoke.

   - Установите флажок **Транзитное устройство CPE**, чтобы разрешить другим устройствам устанавливать туннели через выбранное устройство. По умолчанию флажок снят.

   - В поле **Топологические теги** введите топологический тег и нажмите на кнопку добавления кнопка в виде знака плюс. Устройства с одинаковыми топологическими тегами устанавливают прямые туннели между собой и образуют топологию. Одному устройству CPE можно добавить несколько топологических тегов.

     Вы можете удалить назначенный тег, нажав на кнопку удаления рядом с ним.

4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Настройка транспортных путей

Вы можете настраивать параметры используемых транспортных путей следующим образом:

- В разделе **Сегменты** – конфигурация транспортных путей, указанная в сегменте, переписывает конфигурацию на всех входящих в него устройствах.

- В подразделе **Шаблоны CPE** – конфигурация транспортных путей, указанная в шаблоне, применяется ко всем использующим его устройствам.

- В подразделе **Устройства CPE** – конфигурация транспортных путей, указанная на отдельном устройстве, переписывает конфигурацию, унаследованную из шаблона. На отдельном устройстве невозможно изменить значение коэффициента разброса стоимости (англ. cost variance multiplier).

Чтобы указать параметры транспортных путей:

1. Перейдите к настройке транспортных путей, выполнив одно из следующих действий:

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Сегменты**, нажмите на кнопку **Управление** рядом с сегментом, в котором требуется указать параметры транспортных путей, и в раскрывающемся списке выберите **Изменить**.

   - В области настройки шаблона CPE или отдельного устройства выберите вкладку **Multipathing**.

2. Настройте параметры транспортных путей, выполнив следующие действия:

   - 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.

   - 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 16. По умолчанию указано значение `2`.

- 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 он мог быть добавлен в сегмент. Диапазон значений: от 1 до 10. По умолчанию указано значение `10`.

  Значение этого коэффициента невозможно изменить на отдельных устройствах CPE.

- Установите флажок **Включить балансировку трафика с учетом веса**, чтобы трафик распределялся по транспортным путям примерно пропорционально значению атрибута веса (Path.weight). Если флажок снят, трафик распределяется равномерно и значение атрибута веса для всех транспортных путей равно 1. По умолчанию флажок установлен.

3. Выполните одно из следующих действий:

   - Если вы настраивали транспортные пути в разделе **Сегменты**, нажмите на кнопку **Сохранить**.

   - Если вы настраивали транспортные пути в подразделе **Шаблоны CPE** или **Устройства CPE**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства.

Создание транспортного пути Manual-TE

При создании транспортных путей Manual-TE требуется вручную указать туннели, через которые он будет проходить от устройства CPE (далее также коммутатор) в начале сегмента до коммутатора в конце сегмента. Поддерживается создание двух типов таких транспортных путей:

- Полностью определенные транспортные пути, в которых указывается каждый коммутатор 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 один или несколько промежуточных коммутаторов 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 добавлять транспортные пути Manual-TE в транспортные сервисы.

Примеры возможных транспортных путей Manual-TE:
В примерах ниже используется сокращение Sw (от англ. switch – коммутатор). После номера коммутатора через двоеточие указывается 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 дополнительном меню настройки веб-интерфейса перейдите в раздел **Сегменты**.

2. Нажмите на кнопку **Управление** рядом с сегментом, внутри которого требуется создать транспортный путь Manual-TE, и в раскрывающемся списке выберите **Изменить**.

3. В открывшемся окне нажмите на кнопку **+ Добавить транспортный путь Manual-TE**.

4. В открывшемся окне настройте параметры транспортного пути Manual-TE, выполнив следующие действия:

   - В поле **Имя** ведите имя транспортного пути Manual-TE.

   - В поле **Максимум хопов** введите максимальное количество участков в транспортном пути (или хопов между началом и концом сегмента). Диапазон значений: от 1 до 8. По умолчанию указано значение 4.

5. Настройте параметры участка транспортного пути Manual-TE, выполнив следующие действия:

   - В раскрывающемся списке **От** слева выберите начальный коммутатор участка.

   - При необходимости в раскрывающемся списке **Порт** слева выберите NNI (network-to-network interface) начального коммутатора участка. По умолчанию выбрано значение **AUTO** и интерфейс определяется автоматически.

   - В раскрывающемся списке **До** справа выберите конечный коммутатор участка.

   - При необходимости в раскрывающемся списке **Порт** справа выберите NNI (network-to-network interface) конечного коммутатора участка. По умолчанию выбрано значение **AUTO** и интерфейс определяется автоматически.

   Существуют следующие ограничения:

   - Если в транспортном пути не создано ни одного участка, в качестве начального коммутатора можно выбрать только начальный коммутатор сегмента.

   - Если в транспортном пути создан хотя бы один участок, в качестве начального коммутатора можно выбрать только конечный коммутатор последнего участка.

   - Если для начального коммутатора участка в раскрывающемся списке **Порт** выбрано значение **AUTO**, в качестве конечного коммутатора можно выбрать любой коммутатор в домене, за исключением тех, что используются в других участках. При этом для конечного коммутатора участка в раскрывающемся списке **Порт** автоматически выбирается значение **AUTO**. Таким образом, в участке используется транспортный путь Auto-SPF.

   - Если для начального коммутатора участка в раскрывающемся списке **Порт** выбран NNI, в качестве конечного коммутатора можно выбрать только коммутатор, до которого от NNI построен туннель. При этом для конечного коммутатора участка в раскрывающемся списке **Порт** автоматически выбирается NNI, до которого построен туннель. Таким образом, в участке используется указанный между двумя коммутаторами туннель.

6. Нажмите на кнопку **Добавить**, чтобы добавить участок в транспортный путь Manual-TE.

   Количество хопов в транспортном пути Manual-TE увеличится на один, и в столбце **Стоимость** отобразится стоимость участка, которая складывается из стоимости всех добавленных в него туннелей. Вы не можете добавлять новые участки, если достигнуто максимальное количество участков в транспортном пути.

   Вы можете удалить участок, нажав на кнопку **Удалить** рядом с ним.

7. Нажмите на кнопку **Создать**.

Произойдет следующая проверка: конечный коммутатор последнего участка должен совпадать с конечным коммутатором сегмента, в котором создается транспортный путь Manual-TE. При успешной проверке транспортный путь Manual-TE отобразится в таблице **Транспортные пути сегмента**, а в столбце **Стоимость** отобразится стоимость транспортного пути, которая складывается из стоимости всех добавленных в него участков.

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 обеспечивают следующие компоненты:

- *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 одним из созданных вами классов.

- *QoS-правила* – ограничивают скорость передачи трафика, обрабатываемого создаваемыми классификаторами.

- *Ограничения* – используются в транспортных сервисах для соблюдения SLA. Вы можете создавать два типа ограничений:

  - *Manual TE* – используются для добавления транспортных путей Manual TE в транспортные сервисы. Сначала в такое ограничение добавляются транспортные пути Manual-TE, после чего оно используется в одном из транспортных сервисов. Вы можете создать ограничение, которое в случае недоступности добавленных в него транспортных путей Manual-TE позволяет транспортному сервису использовать транспортный путь Auto-SPF.

  - *Пороговые ограничения* – используются для построения транспортных путей Auto-TE. Сначала в таком ограничении указываются определенные показатели мониторинга туннеля, после чего оно используется в одном из транспортных сервисов.

    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, отличающимся низким показателем потерь пакетов.

  - *Правила классификации трафика* – используются для определения в общем потоке данных трафика с определенными значениями полей заголовков уровней L2 – L4, а также трафика указанных приложений.

    Для каждого правила классификации трафика указывается порядковый номер и выбирается действие по умолчанию, разрешающее или запрещающее дальнейшую маршрутизацию трафика. Созданные правила добавляются в фильтры трафика.

  - *Фильтры трафика* используются для выполнения следующих задач:

- обеспечение безопасности путем блокирования избыточного или потенциально опасного трафика;
- классификация трафика;
- соблюдение требований SLA для приложений.

Каждый фильтр состоит из одного или нескольких правил классификации трафика.

На WAN- и LAN-интерфейсах SD-WAN может использоваться не более 8 очередей трафика. Для каждой очереди требуется указать минимальную и максимальную скорость передачи в процентном выражении 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 передачи. Верхнее ограничение максимальной скорости передачи для более приоритетных очередей необходимо, чтобы предоставить доступ к полосе пропускания трафику из менее приоритетных очередей.

Операторы связи (англ. service providers) могут использовать разные QoS-политики для маркировки очередей в своих сетях и выполнения требований SLA для пропуска клиентского трафика. В результате при одновременном подключении к каналам передачи данных разных операторов связи устройства CPE должны иметь возможность гибкой маркировки трафика разных очередей для каждого WAN-интерфейса. Поэтому настройка шейпинга исходящего трафика на WAN-интерфейсах расширена возможностью изменять значение ToS.

Изменяются только значения ToS внешних (туннельных) заголовков пакетов трафика, исходящих из WAN-интерфейсов. Значения ToS внутренних заголовков пакетов трафика остаются не измененными.

Вы можете настроить очереди для WAN-интерфейсов SD-WAN при создании. В связи с тем, что сейчас Kaspersky SD-WAN не поддерживает создание LAN-интерфейсов SD-WAN, очереди можно настроить только для уже существующих LAN-интерфейсов.

Создание и изменение класса трафика

Вы можете создать от 4 до 8 классов трафика при настройке шаблона экземпляра SD-WAN. Когда вы развернули экземпляр SD-WAN с помощью шаблона, изменить параметры классов трафика или создать новые невозможно.

Классы трафика, созданные по умолчанию, подходят для большинства схем развертывания решения Kaspersky SD-WAN, и мы не рекомендуем изменять их.

Чтобы создать или изменить класс трафика:

1. В области настройки шаблона экземпляра SD-WAN выберите вкладку **Классы трафика**.
2. Нажмите на кнопку **Изменить**.
3. В открывшемся окне нажмите на кнопку **+ Добавить класс трафика** и настройте параметры класса трафика, выполнив следующие действия:
   - В столбце **Имя** укажите имя для класса трафика.

- 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.

- В столбце **KOver** выберите коэффициент переподписки скорости передачи трафика. Каждому классу трафика доступна скорость передачи в процентном выражении от общей скорости, заданной для всего интерфейса. Коэффициент переподписки определяет, во сколько раз может быть увеличена скорость передачи трафика, если общая скорость используется не полностью.

- Установите флажок **Не учитывать при расчете транспортного пути**, чтобы не учитывать доступную классу трафика скорость при расчете маршрута. Если флажок установлен, вы не можете выбрать для класса трафика коэффициент **KOver**. По умолчанию флажок установлен рядом с последним в таблице классом трафика (**Best Effort**).

- 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**).

- В раскрывающемся списке **Класс управляющего трафика** выберите класс, в который требуется помещать управляющий трафик. По умолчанию выбран первый в таблице класс трафика (**Network Control**).

  Управляющий трафик – это сетевой трафик, используемый 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.

- 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**.

4. Нажмите на кнопку **OK**.

   Класс трафика отобразится в таблице.

5. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона экземпляра SD-WAN.

Создание классификатора трафика

Вы можете создавать классификаторы трафика в разделе **QoS** или подразделе **Шаблоны экземпляров SD-WAN** веб-интерфейса оркестратора.

Чтобы создать классификатор трафика:

1. Откройте список классификаторов трафика, выполнив одно из следующих действий:

   - В области настройки шаблона экземпляра SD-WAN выберите вкладку **Классификаторы**.

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **QoS** и выберите вкладку **Классификаторы**.

2. Нажмите на кнопку **+ Добавить классификатор трафика**.

3. В открывшемся окне настройте параметры классификатора трафика, выполнив следующие действия:

- В поле **Имя** введите имя классификатора трафика.
- В списке **Типы** выберите одно из следующих значений:
  - **Trust** – классификатор, доверяющий DSCP-значениям, выставленным в полях заголовков пакетов трафика. Это значение выбрано по умолчанию. *DSCP-значения* – это 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.

    При выборе этого значения вам нужно установить соответствие между классами трафика и DSCP-значениями в блоке **Сопоставление классов трафика** снизу.
  - **Untrust** – классификатор, не доверяющий DSCP-значениям, выставленным в полях заголовков пакетов трафика.

    При выборе этого значения вам нужно выбрать класс для всего обрабатываемого классификатором трафика в раскрывающемся списке **Класс трафика** снизу.

4. Если в списке **Типы** вы выбрали **Trust**, установите соответствие между классами и DSCP-значениями в заголовках пакетов трафика, выполнив следующие действия:
   a. В столбце **Класс трафика** выберите класс, в который требуется помещать трафик.
   b. В столбце **Метка обслуживания** нажмите на кнопку **Выбрать** рядом с заголовком пакета, который должен содержать требуемое DSCP-значение.
   c. Установите флажки рядом с DSCP-значениями, которые должны быть в заголовке пакета для помещения трафика в выбранный класс.
   d. Нажмите на кнопку **OK**.
5. Если в списке **Типы** вы выбрали **Untrust**, в раскрывающемся списке **Класс трафика** выберите класс, в который требуется помещать весь трафик.
6. Нажмите на кнопку **Применить**.

   Классификатор трафика отобразится в таблице. Вы можете выполнить одно из следующих действий с классификатором трафика, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:
   - Изменить параметры классификатора трафика, выбрав **Изменить**.
   - Удалить классификатор трафика, выбрав **Удалить**.
7. При создании классификатора трафика в подразделе **Шаблоны экземпляров SD-WAN** нажмите на кнопку **Сохранить** вверху справа, чтобы сохранить конфигурацию шаблона.

Создание QoS-правила

Вы можете создавать QoS-правила в разделе **QoS** или подразделе **Шаблоны экземпляров SD-WAN** веб-интерфейса оркестратора.

Чтобы создать QoS-правило:

1. Откройте список QoS-правил, выполнив одно из следующих действий:

   - В области настройки шаблона экземпляра SD-WAN выберите вкладку **QoS-правила**.
   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **QoS** и выберите вкладку **QoS-правила**.

2. Нажмите на кнопку **+ Добавить QoS-правило**.

3. В открывшемся окне настройте параметры QoS-правила, выполнив следующие действия:

   - В поле **Имя** введите имя QoS-правила.
   - В раскрывающемся списке **Классификатор** выберите классификатор трафика, который требуется использовать в QoS-правиле.
   - Установите флажок **Без ограничения**, чтобы не ограничивать скорость передачи трафика, обрабатываемого выбранным ранее классификатором. По умолчанию флажок установлен.

4. При необходимости снимите флажок **Без ограничения** и установите ограничение скорости передачи трафика, выполнив следующие действия:

   - В поле **MBR** введите максимальную скорость передачи трафика (англ. Maximum Bit Rate). По умолчанию указано значение `1`.
   - В раскрывающемся списке **Единицы измерения** выберите единицы измерения максимальной скорости передачи трафика:
     - **Кбит/с** – это значение выбрано по умолчанию.
     - **Мбит/с**.
     - **Гбит/с**.
   - Если вы выбрали классификатор с типом **Trust** в раскрывающемся списке **Классификатор**, укажите процент от общей скорости передачи трафика, доступный каждому классу в столбце **Максимальная зарезервированная скорость (%)**. Сумма значений, указанных для каждого класса, должна быть равна 100.

5. Нажмите на кнопку **Применить**.

   QoS-правило отобразится в таблице. Вы можете выполнить одно из следующих действий с QoS-правилом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

   - Изменить параметры QoS-правила, выбрав **Изменить**.
   - Удалить QoS-правило, выбрав **Удалить**.

6. При создании QoS-правила в подразделе **Шаблоны экземпляров SD-WAN** нажмите на кнопку **Сохранить** вверху справа, чтобы сохранить конфигурацию шаблона.

Создание ограничения Manual-TE

Перед выполнением этой инструкции требуется создать транспортные пути Manual-TE.

Чтобы создать ограничение Manual-TE:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Ограничения**.
2. Нажмите на кнопку **+ Добавить ограничение Manual-TE**.
3. В открывшемся окне настройте параметры ограничения, выполнив следующие действия:
   - В поле **Имя** введите имя ограничения Manual-TE.
   - Установите флажок **Использовать транспортный 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.
   - Установите флажок **Игнорировать, если транспортный путь с ограничением не найден** рядом с транспортными путями Manual-TE, чтобы разрешить использование транспортного пути Auto-SPF в случае их недоступности. Флажок можно установить только рядом с транспортными путями, рядом с которыми установлен флажок **Использовать транспортный путь Manual-TE**. По умолчанию флажки сняты и для всех транспортных путей запрещено использование Auto-SPF в качестве альтернативы.
4. Нажмите на кнопку **Сохранить**.

Ограничение отобразится в таблице. Теперь его можно указать в параметрах транспортного сервиса, чтобы добавить в этот сервис содержащиеся в ограничении транспортные пути Manual-TE.

Вы можете выполнить одно из следующих действий с ограничением, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры ограничения, выбрав **Изменить**.
- Удалить ограничение, выбрав **Удалить**.

Создание порогового ограничения

Перед выполнением этой инструкции требуется включить мониторинг на туннелях.

Чтобы создать пороговое ограничение:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Ограничения** и выберите вкладку **Пороговые ограничения**.
2. Нажмите на кнопку **+ Добавить пороговое ограничение**.
3. В открывшемся окне настройте параметры ограничения, выполнив следующие действия:
   - В поле **Имя** введите имя порогового ограничения.
   - 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 флажки сняты и ни один показатель мониторинга не используется для исключения туннелей
   - Установите флажок **Игнорировать, если транспортный 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 флажки сняты и ограничение исключает из расчета транспортного пути Auto-TE все туннели, на которых достигнуты пороговые значения выбранных вами показателей мониторинга.

4. Нажмите на кнопку **Сохранить**.

Ограничение отобразится в таблице. Теперь его можно указать в параметрах транспортного сервиса, чтобы использовать при автоматическом расчете транспортного пути.

Вы можете выполнить одно из следующих действий с ограничением, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры ограничения, выбрав **Изменить**.
- Удалить ограничение, выбрав **Удалить**.

Создание правила классификации трафика

Чтобы создать правило классификации трафика:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Фильтр** и выберите вкладку **Правила**.
2. Вверху справа нажмите на кнопку **+ Добавить правило**.
3. В открывшемся окне в поле **Имя** введите имя правила классификации трафика.
4. На вкладке **L2-поля** установите флажки рядом с L2-полями, значения которых правило должно использовать для определения трафика из общего потока данных. Установив флажок рядом с полем, вам нужно ввести или выбрать требуемое значение справа. 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**.

5. Выберите вкладку **L3-поля** и установите флажки рядом с L3-полями, значения которых правило должно использовать для определения трафика из общего потока данных. Установив флажок рядом с полем, вам нужно ввести или выбрать требуемое значение справа. 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**.

6. Выберите вкладку **L4-поля** и установите флажки рядом с L4-полями, значения которых правило должно использовать для определения трафика из общего потока данных. Установив флажок рядом с полем, вам нужно ввести или выбрать требуемое значение справа. Вы можете использовать значения следующих полей для определения трафика:

   - **IP-протокол**.
   - **Список портов источника**.
   - **Список портов назначения**.
   - **Номер типа ICMP**.

7. Выберите вкладку **DPI** и выберите приложение, трафик которого правило должно определять из общего потока данных, выполнив следующие действия:

   a. Установите флажок **Приложение**.

   b. В раскрывающемся списке справа выберите требуемое приложение.

   > Классификация с помощью DPI (Deep Packet Inspection) не поддерживается для трафика, сгенерированного устройствами CPE.

8. Нажмите на кнопку **Создать**.

Правило классификации трафика отобразится в таблице. Теперь его можно использовать при создании фильтра трафика.

Пример созданного правила классификации трафика:
Вы можете создать правило классификации трафика со следующими характеристиками:

- 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.

Вы можете выполнить одно из следующих действий с правилом классификации трафика, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры правила классификации трафика, выбрав **Изменить**.
- Удалить правило классификации трафика, выбрав **Удалить**.

Создание фильтра трафика

Перед выполнением этой инструкции требуется создать как минимум одно правило классификации трафика.

Чтобы создать фильтр трафика:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Фильтр**.
2. Вверху справа нажмите на кнопку **+ Добавить фильтр**.
3. В открывшемся окне в поле **Имя** введите имя фильтра трафика.
4. Настройте параметры правила классификации трафика, которое требуется добавить в фильтр, выполнив следующие действия:
   - В поле **Порядковый номер** 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`.
   - В раскрывающемся списке **Правило** выберите правило классификации трафика, которое требуется добавить в фильтр.
   - 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.

5. Добавьте правило классификации трафика в фильтр, нажав на кнопку **Добавить**.
6. В раскрывающемся списке **Действие по умолчанию (Посл=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.
7. Нажмите на кнопку **Сохранить**.

Фильтр трафика отобразится в таблице. Теперь его можно использовать при создании транспортных сервисов.

Вы можете выполнить одно из следующих действий с фильтром трафика, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры фильтра трафика, выбрав **Изменить**.
- Удалить фильтр трафика, выбрав **Удалить**.

Транспортные сервисы P2P, P2M, M2M, IP multicast и L3 VPN

Транспортные сервисы строятся поверх сегментов и используются для передачи трафика между сервисными интерфейсами. Kaspersky SD-WAN поддерживает создание следующих типов транспортных сервисов:

- *P2P* (Point-to-Point, E-line в классификации MEF, далее также P2P-сервис) – используется для передачи трафика между двумя сервисными интерфейсами устройств CPE, где первый сервисный интерфейс является источником (далее также интерфейс-источник), а второй является назначением (далее также интерфейс-назначение).
- *P2M* (Point-to-Multipoint, E-tree в классификации MEF, далее также P2M-сервис) – используется для передачи трафика между двумя и более сервисными интерфейсами устройств CPE. В рамках этого транспортного сервиса каждому сервисному интерфейсу назначается одна из следующих ролей:
  - **Root** – трафик, поступающий в сервисный интерфейс, может быть отправлен на сервисный интерфейс с любой ролью. Эту роль требуется назначить как минимум одному сервисному интерфейсу.
  - **Leaf** – трафик, поступающий в сервисный интерфейс, может быть отправлен только на сервисный интерфейс с ролью Root.

  Поддерживается передача кадров, соответствующих стандартам IEEE 802.1Q и 802.1AD.

- *M2M* (Multipoint-to-Multipoint, E-LAN в классификации MEF, далее также M2M-сервис) – используется для передачи трафика между двумя и более сервисными интерфейсами устройств CPE. Этот транспортный сервис является распределенным bridge-доменом, который использует механизм изучения MAC-адресов (англ. MAC learning) для заполнения MAC-таблицы на контроллере SD-WAN.

На каждом устройстве CPE, сервисные интерфейсы которого добавлены в транспортный сервис, организуется отдельный bridge-домен. Помимо общей таблицы MAC-адресов на контроллере SD-WAN, на каждом устройстве CPE содержатся отдельные таблицы MAC-адресов.

- *IP multicast* (далее также IP multicast-сервис) – используется для передачи multicast-трафика между двумя и более сервисными интерфейсами устройств CPE. В рамках этого транспортного сервиса строится дерево распространения multicast-трафика внутри домена, и корнем этого дерева является сервисный интерфейс, к которому подключен источник трафика (далее также интерфейс-источник).

  Интерфейс-источник передает multicast-трафик на сервисные интерфейсы, к которым подключены подписчики (далее также интерфейсы-подписчики). Интерфейсы-подписчики могут подключаться к multicast-группам с адресом назначения из диапазона IP-адресов 224.0.0.0/4 по протоколу IGMPv2/v3.

  Трафик передается через транспортный сервис IP multicast как Ethernet-кадры с IP payload без дополнительной инкапсуляции.

- *L3 VPN* (далее также L3 VPN-сервис) – используется для обеспечения L3-маршрутизации между разными сетями с возможностью указания статических маршрутов. В рамках этого транспортного сервиса поверх сервисных интерфейсов устройств CPE или транспортных сервисов M2M создаются L3-интерфейсы, которые используются для передачи трафика.

  Поддерживается топология Full-Mesh, в которой допускается взаимодействие между любыми сетями.

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.

Создание P2P

Перед выполнением этой инструкции требуется выполнить следующие действия:

- активировать устройства CPE;
- создать сервисные интерфейсы.

Чтобы создать транспортный сервис P2P:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **P2P**.
2. Нажмите на кнопку **+ Добавить P2P**.
3. В открывшемся окне настройте параметры P2P-сервиса, выполнив следующие действия:
   - В поле **Имя** введите имя транспортного сервиса.
   - В раскрывающемся списке **Ограничение** выберите ограничение (Manual-TE или пороговое), которое требуется добавить в транспортный сервис.
   - В раскрывающемся списке **Режим балансировки** выберите одно из следующих значений:

- **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.

Режим балансировки используется для равномерного распределения трафика по туннелям для предотвращения перегрузки отдельных туннелей и последующего возникновения проблем с производительностью у пользователей.

- В поле **Описание** введите краткое описание P2P-сервиса.

- В раскрывающихся списках **Коммутатор** и **Порт** слева выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как интерфейс-источник.

- В раскрывающихся списках **Коммутатор** и **Порт** справа выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как интерфейс-назначение.

- Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить в раскрывающихся списках **Порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.

- Установите флажок **Переключить сервисные интерфейсы**, чтобы поменять местами значения, выбранные в раскрывающемся списке **Порт** для интерфейса-источника и интерфейса-назначения. По умолчанию флажок снят.

- Установите флажок **Резервный сервисный интерфейс**, чтобы добавить резервный интерфейс-источник. Использование резервного сервисного интерфейса позволяет продолжать передачу данных в случае выхода из строя основного сервисного интерфейса. По умолчанию флажок снят. Если флажок установлен, вам нужно указать параметры резервного сервисного интерфейса, выполнив следующие действия:

  - В раскрывающихся списках **Резервный коммутатор** и **Резервный порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как резервный.

  - Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить в раскрывающемся списке **Резервный порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.

  Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.

- В раскрывающихся списках **Входящий фильтр** слева и справа выберите фильтр трафика для интерфейса-источника и интерфейса-назначения.

- В раскрывающемся списке **QoS** выберите правило качества обслуживания для интерфейса-источника.

- Установите флажок **Транслировать статус интерфейса**, чтобы отслеживать состояние обоих сервисных интерфейсов, и при выключении одного из них автоматически выключать второй. По умолчанию флажок снят. Флажок невозможно установить, если установлен флажок **Резервный сервисный интерфейс**.

Если 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.

4. Нажмите на кнопку **Сохранить**.

P2P-сервис отобразится в таблице. Вы можете выполнить одно из следующих действий с транспортным сервисом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры транспортного сервиса, выбрав **Изменить**.
- Удалить транспортный сервис, выбрав **Удалить**. Если требуется удалить добавленные в сервис сервисные интерфейсы, в окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.
- Просмотреть статистику работы транспортного сервиса, выбрав **Статистика**.
- Настроить отображение устройств в топологии транспортного сервиса, выбрав **Топология**.
- Переконфигурировать транспортный сервис, выбрав **Повторная инициализация**. Переконфигурация может потребоваться в случае, если при функционировании сервиса возникла проблема (например с сетевым подключением) или в текущую конфигурацию были внесены изменения, которые требуют перезагрузки сервиса.

  Откроется окно с сообщением об успешном перезапуске транспортного сервиса. При успешном обновлении контроллер SD-WAN добавит сервис на все устройства CPE, которые ранее использовались в этом сервисе.

Создание P2M

Перед выполнением этой инструкции требуется выполнить следующие действия:

- активировать устройства CPE;
- создать сервисные интерфейсы;
- определить топологию транспортного сервиса с назначением ролей сервисным интерфейсам.

Чтобы создать транспортный сервис P2M:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **P2M**.
2. Нажмите на кнопку **+ Добавить P2M**.
3. В открывшемся окне настройте параметры P2M-сервиса, выполнив следующие действия:
   - В поле **Имя** введите имя транспортного сервиса.
   - В раскрывающемся списке **Ограничение** выберите ограничение (Manual-TE или пороговое), которое требуется добавить в транспортный сервис.
   - В раскрывающемся списке **Режим балансировки** выберите одно из следующих значений:

- **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.

Режим балансировки используется для равномерного распределения трафика по туннелям для предотвращения перегрузки отдельных туннелей и последующего возникновения проблем с производительностью у пользователей.

- В раскрывающемся списке **Режим изучения MAC** выберите действие, которое требуется применить к серии кадров после того, как первый кадр из этой серии 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.

- В поле **Время жизни MAC, сек** введите время в секундах, в течение которого записи хранятся в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 10 до 65535. По умолчанию указано значение `300`.

- В раскрывающемся списке **При переполнении 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.

- В поле **Размер таблицы MAC-адресов** введите максимальное количество записей в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 0 до 65535. Вы можете ввести `0`, чтобы не ограничивать количество записей. По умолчанию указано значение `100`.

- В раскрывающемся списке **Режим работы транспортного сервиса** 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.

- В поле **Описание** введите краткое описание транспортного сервиса.

4. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

5. Настройте параметры сервисного интерфейса, выполнив следующие действия:

   - В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется добавить в транспортный сервис.

   - Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить в раскрывающемся списке **Порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.

   - В раскрывающемся списке **QoS** выберите правило качества обслуживания для сервисного интерфейса.

   - В раскрывающемся списке **Входящий фильтр** выберите фильтр трафика для сервисного интерфейса.

   - В раскрывающемся списке **Роль** выберите роль сервисного интерфейса:

     - **Leaf**.

     - **Root**.

   - Установите флажок **Резервный сервисный интерфейс**, чтобы добавить резервный сервисный интерфейс. Использование резервного сервисного интерфейса позволяет продолжать передачу данных в случае выхода из строя основного сервисного интерфейса. По умолчанию флажок снят. Если флажок установлен, вам нужно указать параметры резервного сервисного интерфейса, выполнив следующие действия:

     - В раскрывающихся списках **Резервный коммутатор** и **Резервный порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как резервный.

     - Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить в раскрывающемся списке **Резервный порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.

     Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.

   - Установите флажок **Default Forwarding Interface**, чтобы назначить роль DFI сервисному интерфейсу. Флажок невозможно установить, если в раскрывающемся списке **Роль** вы выбрали **Leaf** для сервисного интерфейса.

6. Нажмите на кнопку **+ Добавить**, чтобы добавить сервисный интерфейс в транспортный сервис.

   Сервисный интерфейс отобразится в нижней части окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.

7. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

8. Настройте параметры OpenFlow-интерфейсов, выполнив следующие действия:

   - В раскрывающемся списке **Группа** выберите группу OpenFlow-интерфейсов, которую требуется добавить. Поверх каждого OpenFlow-интерфейса в группе автоматически создается сервисный интерфейс, который в свою очередь добавляется в транспортный сервис.

   - В раскрывающемся списке **QoS** выберите правило качества обслуживания для сервисных интерфейсов, созданных поверх OpenFlow-интерфейсов.

   - 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.

   - В раскрывающемся списке **Роль** выберите роль для сервисных интерфейсов, автоматически созданных поверх OpenFlow-интерфейсов:

     - **Leaf**.

     - **Root**.

9. Нажмите на кнопку **+ Добавить**, чтобы добавить группу OpenFlow-интерфейсов в транспортный сервис.

   Автоматически созданные сервисные интерфейсы отобразятся в нижней части окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.

10. Нажмите на кнопку **Сохранить**.

P2M-сервис отобразится в таблице. Вы можете выполнить одно из следующих действий с транспортным сервисом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры транспортного сервиса, выбрав **Изменить**.

- Удалить транспортный сервис, выбрав **Удалить**. Если требуется удалить добавленные в сервис сервисные интерфейсы, в окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

- Просмотреть статистику работы транспортного сервиса, выбрав **Статистика**.

- Просмотреть MAC-таблицу транспортного сервиса, выбрав **Таблица MAC-адресов**. Вы также можете выполнить одно из следующих действий в MAC-таблице:

  - Найти MAC-адрес, введя его имя и нажав на кнопку **Найти по MAC**.

  - Удалить все MAC-адреса, нажав на кнопку **Очистить**.

- Настроить отображение устройств в топологии транспортного сервиса, выбрав **Топология**.

- Переконфигурировать транспортный сервис, выбрав **Повторная инициализация**. Переконфигурация может потребоваться в случае, если при функционировании сервиса возникла проблема (например с сетевым подключением) или в текущую конфигурацию были внесены изменения, которые требуют перезагрузки сервиса.

Откроется окно с сообщением об успешном перезапуске транспортного сервиса. При успешном обновлении контроллер SD-WAN добавит сервис на все устройства CPE, которые ранее использовались в этом сервисе.

Создание M2M

Перед выполнением этой инструкции требуется выполнить следующие действия:

- активировать устройства CPE;
- создать сервисные интерфейсы.

Чтобы создать транспортный сервис M2M:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **M2M**.
2. Нажмите на кнопку **+ Добавить M2M**.
3. В открывшемся окне настройте параметры M2M-сервиса, выполнив следующие действия:
   - В поле **Имя** введите имя транспортного сервиса.
   - В раскрывающемся списке **Ограничение** выберите ограничение (Manual-TE или пороговое), которое требуется добавить в транспортный сервис.
   - В раскрывающемся списке **Режим балансировки** выберите одно из следующих значений:
     - **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.

     Режим балансировки используется для равномерного распределения трафика по туннелям для предотвращения перегрузки отдельных туннелей и последующего возникновения проблем с производительностью у пользователей.
   - В раскрывающемся списке **Режим изучения MAC** выберите действие, которое требуется применить к серии кадров после того, как первый кадр из этой серии 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.

- В поле **Время жизни MAC, сек** введите время в секундах, в течение которого записи хранятся в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 10 до 65535. По умолчанию указано значение `300`.
- В раскрывающемся списке **При переполнении 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.
- В поле **Размер таблицы MAC-адресов** введите максимальное количество записей в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 0 до 65535. Вы можете ввести `0`, чтобы не ограничивать количество записей. По умолчанию указано значение `100`.
- В поле **Описание** введите краткое описание транспортного сервиса.

4. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

5. Настройте параметры сервисного интерфейса, выполнив следующие действия:

- В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется добавить в транспортный сервис.
- Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить в раскрывающемся списке **Порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.
- В раскрывающемся списке **QoS** выберите правило качества обслуживания для сервисного интерфейса.
- В раскрывающемся списке **Входящий фильтр** выберите фильтр трафика для сервисного интерфейса.
- Установите флажок **Резервный сервисный интерфейс**, чтобы добавить резервный сервисный интерфейс. Использование резервного сервисного интерфейса позволяет продолжать передачу данных в случае выхода из строя основного сервисного интерфейса. По умолчанию флажок снят. Если флажок установлен, вам нужно указать параметры резервного сервисного интерфейса, выполнив следующие действия:
  - В раскрывающихся списках **Резервный коммутатор** и **Резервный порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как резервный.
  - Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить в раскрывающемся списке **Резервный порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.

Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.

6. Нажмите на кнопку **+ Добавить**, чтобы добавить сервисный интерфейс в транспортный сервис.

Сервисный интерфейс отобразится в нижней части окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.

7. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

8. Настройте параметры OpenFlow-интерфейсов, выполнив следующие действия:

   - В раскрывающемся списке **Группа** выберите группу OpenFlow-интерфейсов, которую требуется добавить. Поверх каждого OpenFlow-интерфейса в группе автоматически создается сервисный интерфейс, который в свою очередь добавляется в транспортный сервис.

   - В раскрывающемся списке **QoS** выберите правило качества обслуживания для сервисных интерфейсов, созданных поверх OpenFlow-интерфейсов.

   - 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.

9. Нажмите на кнопку **+ Добавить**, чтобы добавить группу OpenFlow-интерфейсов в транспортный сервис.

   Автоматически созданные сервисные интерфейсы отобразятся в нижней части окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.

10. Нажмите на кнопку **Сохранить**.

M2M-сервис отобразится в таблице. Вы можете выполнить одно из следующих действий с транспортным сервисом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры транспортного сервиса, выбрав **Изменить**.

- Удалить транспортный сервис, выбрав **Удалить**. Если требуется удалить добавленные в сервис сервисные интерфейсы, в окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

- Просмотреть статистику работы транспортного сервиса, выбрав **Статистика**.

- Просмотреть MAC-таблицу транспортного сервиса, выбрав **Таблица MAC-адресов**. Вы также можете выполнить одно из следующих действий в MAC-таблице:

  - Найти MAC-адрес, введя его имя и нажав на кнопку **Найти по MAC**.

  - Удалить все MAC-адреса, нажав на кнопку **Очистить**.

- Настроить отображение устройств в топологии транспортного сервиса, выбрав **Топология**.

- Переконфигурировать транспортный сервис, выбрав **Повторная инициализация**. Переконфигурация может потребоваться в случае, если при функционировании сервиса возникла проблема (например с сетевым подключением) или в текущую конфигурацию были внесены изменения, которые требуют перезагрузки сервиса.

  Откроется окно с сообщением об успешном перезапуске транспортного сервиса. При успешном обновлении контроллер SD-WAN добавит сервис на все устройства CPE, которые ранее использовались в этом сервисе.

Создание IP multicast

Перед выполнением этой инструкции требуется выполнить следующие действия:

- активировать устройства CPE;
- создать сервисные интерфейсы для источника и подписчика трафика.

Чтобы создать транспортный сервис IP multicast:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **IP multicast**.
2. Нажмите на кнопку **+ Добавить IP multicast**.
3. В открывшемся окне настройте параметры IP multicast-сервиса, выполнив следующие действия:
   - В поле **Имя** введите имя транспортного сервиса.
   - В раскрывающихся списках **Основной коммутатор** и **Основной порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как интерфейс-источник.
   - Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить раскрывающемся списке **Основной порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.
   - В поле **IP источника** введите IP-адрес интерфейса-источника.
   - Установите флажок **Резервный сервисный интерфейс-источник**, чтобы добавить резервный интерфейс-источник. Использование резервного сервисного интерфейса позволяет продолжать передачу данных в случае выхода из строя основного сервисного интерфейса. По умолчанию флажок снят. Если флажок установлен, вам нужно указать параметры резервного сервисного интерфейса, выполнив следующие действия:
     - В раскрывающихся списках **Резервный коммутатор** и **Порт резервного коммутатора** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как резервный.
     - Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить в раскрывающемся списке **Порт резервного коммутатора** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.

       Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.
     - Установите флажок **Переключаться на основной сервисный интерфейс**, чтобы прекращать использование резервного сервисного интерфейса в случае восстановления основного. По умолчанию флажок снят.
     - Установите флажок **Резервное multicast-дерево**, чтобы строить дерево распространения multicast-трафика одновременно на основном и резервном сервисном интерфейсе. При этом пакеты трафика отбрасываются на резервном сервисном интерфейсе, пока основной остается активным. По умолчанию флажок установлен.
   - Установите флажок **IGMP-прокси**, чтобы использовать прокси-сервер IGMP. Эта функция сохраняет передачу трафика на активные multicast-группы, к которым подключен как минимум один сервисный

интерфейс-подписчик. По умолчанию флажок снят.

- В раскрывающемся списке **QoS** выберите правило качества обслуживания для интерфейса-источника.

4. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.
5. Настройте параметры интерфейса-подписчика, выполнив следующие действия:
   - В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, который требуется использовать как интерфейс-подписчик.
   - Установите флажок **Показать используемые сервисные интерфейсы**, чтобы отобразить раскрывающемся списке **Порт** сервисные интерфейсы, которые ранее были добавлены в транспортные сервисы. По умолчанию флажок снят.
6. Нажмите на кнопку **+ Добавить**, чтобы добавить сервисный интерфейс в транспортный сервис.

   Сервисный интерфейс отобразится в нижней части окна. Вы можете удалить сервисный интерфейс, нажав на кнопку **Удалить** рядом с ним.
7. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.
8. Настройте параметры multicast-группы, выполнив следующие действия:
   - В поле **IP-адрес** введите IP-адрес multicast-группы. Диапазон значений: от 224.0.0.0 до 239.255.255.255.
   - В раскрывающемся списке **Маска** выберите маску IP-адреса. Диапазон значений: от 24 до 32.
   - В раскрывающемся списке **GBR** выберите гарантированную скорость передачи (англ. Guaranteed Bit Rate, GBR) для multicast-группы.
9. Нажмите на кнопку **+ Добавить**, чтобы добавить multicast-группу в транспортный сервис.

   Multicast-группа отобразится в нижней части окна. Вы можете удалить multicast-группу, нажав на кнопку **Удалить** рядом с ней.
10. Нажмите на кнопку **Сохранить**.

IP multicast-сервис отобразится в таблице. Вы можете выполнить одно из следующих действий с транспортным сервисом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры транспортного сервиса, выбрав одно из следующих значений:
  - **Изменить сервисные интерфейсы-источники**.
  - **Изменить сервисные интерфейсы-подписчики**.
  - **Изменить multicast-группы**.
- Удалить транспортный сервис, выбрав **Удалить**. При необходимости удалить добавленные в сервис сервисные интерфейсы в окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.
- Просмотреть статистику работы транспортного сервиса, выбрав **Статистика**.

Создание L3 VPN

Перед выполнением этой инструкции требуется выполнить следующие действия:

- активировать устройства CPE;
- создать сервисные интерфейсы или транспортные сервисы M2M.

Чтобы создать транспортный сервис L3 VPN:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **L3 VPN**.
2. Нажмите на кнопку **+ Добавить L3 VPN**.
3. В открывшемся окне настройте параметры L3 VPN-сервиса, выполнив следующие действия:
   - В поле **Имя** введите имя транспортного сервиса.
   - В раскрывающемся списке **Ограничение** выберите ограничение (Manual-TE или пороговое), которое требуется добавить в транспортный сервис.
   - В раскрывающемся списке **Режим балансировки** выберите одно из следующих значений:
     - **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.

     Режим балансировки используется для равномерного распределения трафика по туннелям для предотвращения перегрузки отдельных туннелей и последующего возникновения проблем с производительностью у пользователей.
4. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.
5. В раскрывающемся списке **Режим** выберите тип L3-интерфейса:
   - **M2M Point** – создать L3-интерфейс поверх M2M-сервиса. При выборе этого значения вам нужно выбрать M2M-сервис, поверх которого требуется создать L3-интерфейс, в раскрывающемся списке **Сеть**.
   - **Switch/port point** – создать L3-интерфейс поверх сервисного интерфейса. При выборе этого значения вам нужно настроить параметры сервисного интерфейса, выполнив следующие действия:
     - В раскрывающихся списках **Коммутатор** и **Порт** выберите устройство CPE и созданный на нем сервисный интерфейс, поверх которого требуется создать L3-интерфейс.
     - В поле **VLAN по умолчанию** введите внешнюю VLAN-метку.
     - В раскрывающемся списке **QoS** выберите правило качества обслуживания для сервисного интерфейса.

- В раскрывающемся списке **Входящий фильтр** выберите фильтр трафика для сервисного интерфейса.

6. Настройте параметры L3-интерфейса, выполнив следующие действия:

   - В поле **IP** введите IP-адрес L3-интерфейса.
   - В поле **Длина префикса** введите длину префикса L3-интерфейса. Диапазон значений: от 0 до 32.
   - В поле **MAC** введите MAC-адрес сервисного интерфейса. Вы можете нажать на кнопку **Сгенерировать**, чтобы сгенерировать MAC-адрес.
   - В поле **Время жизни (сек.)** введите время в секундах, в течение которого записи могут храниться в ARP-таблице на контроллере SD-WAN. Диапазон значений: от 1 до 65535. По умолчанию указано значение `200`.
   - Установите флажок **Включить DHCP Relay**, чтобы перенаправлять запрос `DHCPDISCOVER` на сервер или серверы, которые вы сможете указать далее в блоке **Серверы DHCP**.

7. Нажмите на кнопку **+ Добавить**, чтобы создать L3-интерфейс.

   L3-интерфейс отобразится в нижней части окна. Вы можете удалить L3-интерфейс, нажав на кнопку **Удалить** рядом с ним.

8. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

9. Настройте параметры статического маршрута, выполнив следующие действия:

   - В поле **IP** введите IP-адрес узла или сети назначения.
   - В поле **Длина префикса** введите длину префикса узла назначения. Диапазон значений: от 0 до 32.
   - В раскрывающемся списке **SVI** выберите L3-интерфейс для отправки пакетов трафика на узел назначения.
   - В поле **Шлюз** введите IP-адрес шлюза для маршрутизации пакетов трафика.
   - В поле **Метрика** введите метрику статического маршрута. По умолчанию указано значение `0`.

10. Нажмите на кнопку **+ Добавить**, чтобы создать статический маршрут.

    Статический маршрут отобразится в нижней части окна. Вы можете удалить статический маршрут, нажав на кнопку **Удалить** рядом с ним.

11. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

12. При необходимости в блоке **Серверы DHCP** нажмите на кнопку **+ Добавить** и введите IP-адрес DHCP-сервера, чтобы добавить его в транспортный сервис. Вы можете указать несколько серверов, а также удалить сервер, нажав на кнопку удаления рядом с ним.

13. Нажмите на кнопку **Сохранить**.

L3 VPN-сервис отобразится в таблице. Вы можете выполнить одно из следующих действий с транспортным сервисом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры транспортного сервиса, выбрав **Изменить**.

- Удалить транспортный сервис, выбрав **Удалить**. При необходимости удалить добавленные в сервис сервисные интерфейсы в окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

- Переконфигурировать транспортный сервис, выбрав **Повторная инициализация**. Переконфигурация может потребоваться в случае, если при функционировании сервиса возникла проблема (например с сетевым подключением) или в текущую конфигурацию были внесены изменения, которые требуют перезагрузки сервиса.

  Откроется окно с сообщением об успешном перезапуске транспортного сервиса. При успешном обновлении контроллер SD-WAN добавит сервис на все устройства CPE, которые ранее использовались в этом сервисе.

- Просмотреть ARP-таблицу транспортного сервиса, выбрав **ARP-таблица**. Вы также можете создать статическую запись в ARP таблице.

- Просмотреть таблицу маршрутизации транспортного сервиса, выбрав **Таблица маршрутизации**.

Настройка транспортных сервисов в шаблоне CPE

Вы можете добавить транспортные сервисы в шаблон CPE, после чего применить его к требуемым устройствам. В этом случае поверх OpenFlow-интерфейсов, соответствующих LAN-интерфейсам SD-WAN 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 выполнением этой инструкции требуется создать транспортный сервис в дополнительном меню настройки решения.

Чтобы добавить транспортный сервис в шаблоне CPE:

1. В области настройки шаблона CPE выберите вкладку **Транспортные сервисы**.

2. Нажмите на кнопку **+ Добавить транспортный сервис**.

3. В открывшемся окне настройте параметры транспортного сервиса, выполнив следующие действия:

   > Обратите внимание, что все указываемые вами ниже параметры должны совпадать с ранее созданным транспортным сервисом. Например, вам нужно использовать то же самое имя и тип.

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

   - В поле **Имя QoS** введите имя правила качества обслуживания, которое используется в транспортном сервисе.

   - 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.

- В раскрывающемся списке **Тип транспортного сервиса** выберите одно из следующих значений:
  - **P2M**.
  - **M2M**.
  - **L3VPN**.
- В раскрывающемся списке **Инкапсуляция** выберите тип инкапсуляции на сервисном интерфейсе:
  - **Access** – это значение выбрано по умолчанию.
  - **VLAN** – при выборе этого значения вам нужно ввести внешнюю метку VLAN в поле **VLAN ID**. Диапазон значений: от 1 до 4094.
  - **Q-in-Q** – при выборе этого значения вам нужно ввести внешнюю метку VLAN в поле **VLAN ID** и внутреннюю метку VLAN в поле **Внутренний VLAN ID**. Диапазон значений: от 1 до 4094.

4. Если в раскрывающемся списке **Тип транспортного сервиса** вы выбрали **P2M**, в раскрывающемся списке **Роль** выберите роль сервисного интерфейса:
   - **Leaf** – трафик, поступающий в сервисный интерфейс, может быть отправлен только на сервисный интерфейс с ролью Root.
   - **Root** – трафик, поступающий в сервисный интерфейс, может быть отправлен на сервисный интерфейс с любой ролью.
5. Если в раскрывающемся списке **Тип транспортного сервиса** вы выбрали **L3VPN**, введите IP-адрес в поле **IP-адрес** и маску в поле **Маска**.
6. Нажмите на кнопку **Сохранить**.

   Транспортный сервис отобразится в таблице. Вы можете выполнить одно из следующих действий с транспортным сервисом, нажав на соответствующую кнопку рядом с ним в столбце **Действия**.
   - Изменить параметры транспортного сервиса, нажав на кнопку **Изменить**.
   - Удалить транспортный сервис, нажав на кнопку **Удалить**.
7. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона CPE.

Создание статической записи в ARP-таблице транспортного сервиса L3 VPN

Чтобы создать статическую запись в ARP-таблице транспортного сервиса L3 VPN:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **L3 VPN**.
2. Нажмите на кнопку **Управление** рядом с требуемым транспортным сервисом и в раскрывающемся списке выберите **ARP-таблица**.
3. Нажмите на кнопку **+ Добавить статическую ARP-запись**.
4. В открывшемся окне настройте параметры статической записи, выполнив следующие действия:

- В раскрывающихся списках **Коммутатор** и **Сервисный интерфейс** выберите устройство CPE и созданный на нем сервисный интерфейс, для которого требуется назначить соответствие между IP и MAC-адресом.
- В поле **IP-адрес** введите IP-адрес сервисного интерфейса.
- В поле **IP-адрес** введите MAC-адрес сервисного интерфейса.

5. Нажмите на кнопку **Сохранить**.

Статическая запись отобразится в ARP-таблице. Вы можете выполнить одно из следующих действий со статической записью, нажав на кнопку **Управление** рядом с ней и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры статической записи, выбрав **Изменить**.
- Удалить статическую запись, выбрав **Удалить**.

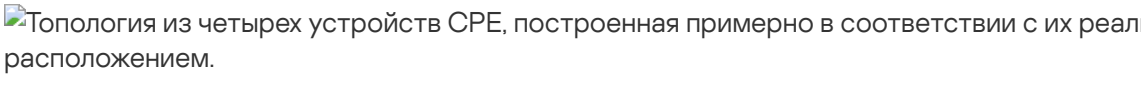
Настройка отображения устройств в топологии транспортного сервиса

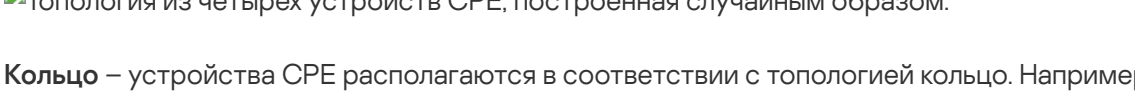
Вы можете настроить отображение устройств в топологии транспортных сервисов P2P, P2M и M2M.

Чтобы настроить отображение устройств в топологии транспортного сервиса:

1. В дополнительном меню настройки веб-интерфейса перейдите в один из следующих разделов:
   - **P2P**.
   - **P2M**.
   - **M2M**.
2. Нажмите на кнопку **Управление** рядом с требуемым транспортным сервисом и в раскрывающемся списке выберите **Топология**.

   Откроется окно с топологией выбранного транспортного сервиса.
3. При необходимости изменить взаимное расположение устройств CPE в топологии используйте кнопки справа вверху:
   - **Вручную** – вы можете вручную изменить взаимное расположение устройств CPE.
   - **Автоматически** – вы можете 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:

       
       Топология из четырех устройств CPE, построенная примерно в соответствии с их реальным расположением.
     - **Случайно** – устройства CPE располагаются случайным образом. Например:

       
       Топология из четырех устройств CPE, построенная случайным образом.
     - **Кольцо** – устройства CPE располагаются в соответствии с топологией кольцо. Например:

Топология кольцо из четырех устройств CPE.

- **Горизонательно** – устройства CPE располагаются горизонтально (в ширину). Например:
  Топология, построенная из четырех устройств CPE горизонательно (в ширину).
- **Концентрически** – устройства CPE располагаются концентрически. Например:
  Концентрическая топология из четырех устройств CPE.
- **Решетка** – устройства CPE располагаются в соответствии с топологией решетка. Например:
  Топология решетка из четырех устройств CPE.

4. Отобразите подписи к устройствам CPE, установив следующие флажки:
   - **Имя**.
   - **IP-адрес**.

   По умолчанию флажки сняты.
5. Отобразите туннели, используемые в сегменте из двух устройств CPE, установив флажок **Сегменты** и выбрав требуемые устройства в раскрывающихся списках снизу или на схеме. По умолчанию флажок снят.
6. Отобразите окно с кнопками управления и дополнительной информацией об устройстве CPE или туннеле, нажав на значок устройства или туннеля.

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 разделе 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.

Указание стоимости туннеля

Вы можете указать стоимость туннелей в разделах **Топология** и **Туннели**, а также в подразделе **Устройства CPE** веб-интерфейса оркестратора.

Чтобы указать стоимость туннеля:

1. Откройте окно настройки стоимости туннеля, выполнив одно из следующих действий:

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Топология**, нажмите на туннель, для которого требуется указать стоимость, и в открывшемся окне нажмите на кнопку **Указать стоимость**.

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, для которого требуется указать стоимость, и в раскрывающемся списке выберите **Указать стоимость**.

   - В области настройки устройства CPE выберите вкладку **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, для которого требуется указать стоимость, и в раскрывающемся списке выберите **Указать стоимость**.

2. В открывшемся окне установите флажок **Переопределить**, чтобы указать стоимость отдельно на туннеле.

3. В поле **Стоимость** введите стоимость туннеля.

4. При необходимости установите флажок **Для обоих туннелей**, чтобы автоматически назначить указанную стоимость аналогичному встречному туннелю.

5. Нажмите на кнопку **Сохранить**.

6. Если вы указали стоимость туннеля в подразделе **Устройства CPE**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства.

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/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.

С помощью этой функции можно решать следующие задачи:

- Обнаружение частых изменений состояния сервисных интерфейсов.
- Перемещение транспортных сервисов, проходящих через нестабильные сервисные интерфейсы, на резервные туннели.
- Исключение сегментов, привязанных к сервисным интерфейсам, из расчета маршрутов для транспортных сервисов.

При включенной функции Dampening 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 10000 раз на определенный промежуток времени). Значение каждого из этих параметров указывается 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 в разделах **Топология** и **Туннели**, а также в подразделе **Устройства CPE** веб-интерфейса оркестратора. По умолчанию функция выключена на туннелях.

Чтобы включить функцию Dampening на туннеле:

1. Откройте окно настройки функции Dampening, выполнив одно из следующих действий:
   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Топология**, нажмите на туннель, на котором требуется включить функцию Dampening, и в открывшемся окне нажмите на кнопку **Dampening**.
   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, на котором требуется включить функцию Dampening, и в раскрывающемся списке выберите **Dampening**.
   - В области настройки устройства CPE выберите вкладку **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, на котором требуется включить функцию Dampening, и в раскрывающемся списке выберите **Dampening**.
2. В открывшемся окне установите флажок **Включить** и настройте параметры функции Dampening, выполнив следующие действия:
   - 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`.

- В поле **Штраф** введите число, которое требуется прибавлять к показателю Penalty при изменении состояния туннеля. По умолчанию указано значение `1`.
- В поле **Порог блокировки** введите значение показателя Penalty, при котором доступ к туннелю ограничивается. По умолчанию указано значение `4`.
- В поле **Интервал обновления (мс)** введите время в миллисекундах, за которое показатель Penalty должен набрать значение, указанное в поле **Порог блокировки**, для ограничения доступа к туннелю. По умолчанию указано значение `120000`.

3. При необходимости нажмите на кнопку **Загрузить статистику**, чтобы отобразить показатели работы функции Dampening на туннеле.
4. Нажмите на кнопку **Сохранить**.
5. Если вы включили функцию Dampening в подразделе **Устройства CPE**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства.

Включение функции Forwarding Error Correction

Функция *Forwarding Error Correction* (далее также FEC) позволяет восстанавливать принимаемые данные на устройстве CPE при наличии потерь пакетов трафика на используемых каналах передачи данных. Восстановление данных обеспечивается избыточным кодированием потока данных на устройстве, находящемся на передающей стороне.

Передающее устройство CPE кодирует поток выходящих в туннель пакетов трафика с добавлением избыточных пакетов. Степень избыточности можно настроить через параметры контроллера SD-WAN или на отдельном туннеле.

Принимающее устройство CPE буферизует принятые через туннель пакеты трафика и декодирует их с восстановлением потерянных пакетов, если это возможно. Общая схема работы функции FEC представлена на рисунке ниже.

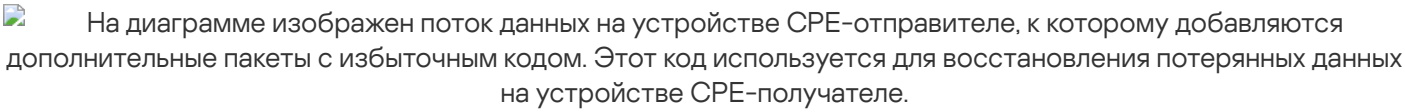

На диаграмме изображен поток данных на устройстве CPE-отправителе, к которому добавляются дополнительные пакеты с избыточным кодом. Этот код используется для восстановления потерянных данных на устройстве CPE-получателе.

Схема работы функции FEC

Использование FEC снижает влияние повышенного показателя потерь пакетов трафика на каналах передачи данных, особенно для UDP-приложений, а также уменьшает количество вызывающих задержки повторных передач пакетов (англ. retransmissions) для TCP-сессий. Мы рекомендуем использовать FEC на так называемых noisy links (или зашумленных туннелях) для уменьшения коэффициента потери пакетов трафика и увеличения скорости TCP-соединений.

Избыточное кодирование потока данных повышает объем передаваемых данных и, соответственно, использование каналов передачи данных. При этом также появляются задержки, вызываемые дополнительной обработкой данных как на передающей, так и на принимающей сторонах.

Вы можете включить функцию FEC на туннелях в разделах **Топология** и **Туннели**, а также в подразделе **Устройства CPE** веб-интерфейса оркестратора. По умолчанию функция выключена на туннелях.

Чтобы включить функцию FEC на туннеле:

1. Откройте окно настройки функции FEC, выполнив одно из следующих действий:

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Топология**, нажмите на туннель, на котором требуется включить функцию FEC, и в открывшемся окне нажмите на кнопку **Параметры FEC/Реорганизации**.

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, на котором требуется включить функцию FEC, и в раскрывающемся списке выберите **Параметры FEC/Реорганизации**.

   - В области настройки устройства CPE выберите вкладку **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, на котором требуется включить функцию FEC, и в раскрывающемся списке выберите **Параметры FEC/Реорганизации**.

2. В открывшемся окне установите флажок **Переопределить**, чтобы настроить FEC отдельно на туннеле.

3. Настройте параметры FEC, выполнив следующие действия:

   - 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.

   - В поле **Тайм-аут** введите максимальное время в миллисекундах, в течение которого пакет трафика может находиться в очереди для применения функции FEC. Диапазон значений: от 1 до 1000.

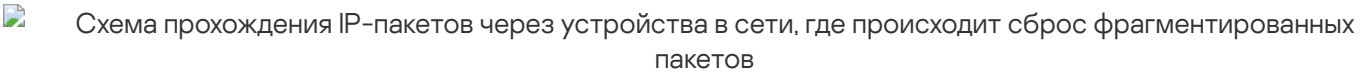
4. Нажмите на кнопку **Сохранить**.

5. Если вы включили функцию FEC на туннеле в подразделе **Устройства CPE**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства. По умолчанию указано значение `0`.

Определение эффективного MTU внутри туннеля

Kaspersky SD-WAN может определять поддерживаемый размер MTU 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 последующем участке 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 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 86400 секунд.

- Вручную по вашему запросу. Вы можете отправить запрос на вычисление MTU на туннеле в разделе **Туннели** и подразделе **Устройства CPE** веб-интерфейса оркестратора.

Вычисленные значения поддерживаемого размера MTU отображаются в столбце **MTU** списка туннелей. Если значение еще не подсчитано, отображается значение *Неизвестно*.

Чтобы вычислить поддерживаемый размер MTU на туннеле вручную:

1. Откройте список туннелей, выполнив одно из следующих действий:

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Туннели**.

   - В области настройки устройства CPE выберите вкладку **Туннели**.

2. Нажмите на кнопку **Управление** рядом с туннелем, на котором вы хотите проверить поддерживаемый размер MTU, 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 (англ. maximum transmission unit) 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.

При включении каждое устройство CPE отправляет два ICMP-запроса со всех WAN-портов на IP-адреса, которые вы указываете в веб-интерфейсе оркестратора при создании интерфейсов SD-WAN, либо в файле настройки контроллера SD-WAN при развертывании решения.

Отправленные ICMP-запросы имеют размер пакета 1600 байт. Если как минимум 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 – проверка фрагментации пакетов на устройстве CPE показала, что на устройстве невозможна передача фрагментированных пакетов.

- Неизвестно – программное обеспечение, установленное на устройстве CPE, не поддерживает проверку возможности фрагментации пакетов.

- Поддерживается – проверка фрагментации пакетов на устройстве CPE показала, что на устройстве возможна передача фрагментированных пакетов.

Результат проверки поддержки фрагментации отображается в веб-интерфейсе оркестратора в подразделе **Устройства CPE** в столбце **Фрагментация**.

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.

> Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

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.

> Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

Используемые ключи регулярно обновляются, чтобы исключить возможность дешифровки переданного трафика третьими лицами 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 не зашифрованный 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 отдельных туннелях. Например, вы можете включить шифрование трафика на устройстве CPE, но выключить его на отдельном туннеле, который построен с использованием этого устройства. При включении или выключении шифрования трафика на туннеле вам нужно одинаковым образом настроить как исходящий, так и входящий туннели.

Шифрование трафика на устройстве CPE

Если на устройстве CPE включено шифрование трафика, по всем туннелям, построенным с его использованием, передается зашифрованный трафик. Исключение составляют случаи, когда вы включаете шифрование трафика на устройстве, но выключаете его на отдельном туннеле.

Вы можете включить или выключить шифрование трафика в шаблоне CPE или на отдельном устройстве По умолчанию шифрование трафика выключено.

Чтобы включить или выключить шифрование трафика на устройстве CPE:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Шифрование**.

2. При настройке отдельного устройства CPE установите флажок **Переопределить** вверху слева, чтобы игнорировать конфигурацию примененного шаблона и получить возможность изменять параметры на выбранной вкладке. По умолчанию флажок снят.

   Если вы настраиваете шаблон CPE, пропустите этот шаг.

3. В раскрывающемся списке **Политика шифрования по умолчанию** выберите **Включено** или **Выключено**.

4. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

Шифрование трафика на туннеле

Если на туннеле включено шифрование трафика, по нему передается зашифрованный трафик. Вы можете включить и выключить шифрование трафика на отдельных туннелях в разделах **Топология** и **Туннели**, а также в подразделе **Устройства CPE** веб-интерфейса оркестратора.

При включении или выключении шифрования трафика на отдельном туннеле вам нужно одинаковым образом настроить аналогичный встречный туннель.

Чтобы включить или выключить шифрование трафика на туннеле:

1. Откройте окно настройки шифрования трафика на туннеле одним из следующих способов:

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Топология**, нажмите на туннель, на котором требуется включить или выключить шифрование трафика, и в открывшемся окне нажмите на кнопку **Включить шифрование туннеля**.

   - В дополнительном меню настройки веб-интерфейса перейдите в раздел **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, на котором требуется включить или выключить шифрование трафика, и в раскрывающемся списке выберите **Включить шифрование туннеля**.

   - В области настройки устройства CPE выберите вкладку **Туннели**, нажмите на кнопку **Управление** рядом с туннелем, на котором требуется включить или выключить шифрование трафика, и в раскрывающемся списке выберите **Включить шифрование туннеля**.

2. В открывшемся окне установите или снимите флажок **Переопределить**, чтобы включить или выключить шифрование трафика отдельно на туннеле. По умолчанию флажок снят.

3. Установите или снимите флажок **Включить шифрование туннеля**. По умолчанию флажок снят.

4. Выполните одно из следующих действий:

   - Если вы включили или выключили шифрование трафика на туннеле в разделе **Топология** или **Туннели**, нажмите на кнопку **Сохранить**.

   - Если вы включили или выключили шифрование трафика на туннеле в подразделе **Устройства CPE**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства.

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 непосредственно 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, которые вы укажете при создании TAP-сервиса. Перед выполнением этой инструкции требуется создать сервисный интерфейс.

Чтобы создать точку назначения трафика:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **TAP**.
2. Нажмите на кнопку **+ Добавить точку назначения**.
3. 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.
4. Нажмите на кнопку **Создать**.

Точка назначения трафика отобразится в таблице. Вы можете удалить точку назначения трафика, нажав на кнопку **Удалить** рядом с ней.

Создание TAP-сервиса

Перед выполнением этой инструкции 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 дополнительном меню настройки веб-интерфейса перейдите в раздел **TAP**.

2. Выберите вкладку **TAP**.

3. Нажмите на кнопку **+ Добавить TAP**.

4. В открывшемся окне настройте параметры TAP-сервиса, выполнив следующие действия:

   - Установите флажок **Зеркалировать**, чтобы зеркалировать на точку назначения трафик, поступающий в точки сбора. При зеркалировании на точку назначения передается копия трафика. Если флажок снят, трафик перенаправляется. По умолчанию флажок снят.

   - В раскрывающемся списке **Режим балансировки** выберите одно из следующих значений:

     - **Per-flow** – балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям. Это значение выбрано по умолчанию.

     - **Per-packet** – балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.

     - **Broadcast**. – пакеты передаются одновременно во все туннели для исключения потерь.

     Режим балансировки используется для равномерного распределения трафика по туннелям для предотвращения перегрузки отдельных туннелей и последующего возникновения проблем с производительностью у пользователей.

   - В раскрывающемся списке **Точка назначения** выберите точку назначения трафика.

   - В раскрывающемся списке **Тип точки сбора** выберите одно из следующих значений:

     - **Сервисный интерфейс** – отдельный сервисный интерфейс.

     - **Транспортный сервис** – сервисный интерфейс, используемый в транспортном сервисе. При выборе этого значения вам нужно выбрать транспортный сервис, в котором используется требуемый сервисный интерфейс, в раскрывающихся списках **Тип транспортного сервиса** и **Транспортный сервис**.

   - В раскрывающемся списке **Точки сбора** выберите сервисные интерфейсы, которые требуется использовать в качестве точек сбора трафика.

5. Нажмите на кнопку **Далее** и выберите правила классификации трафика для точки назначения.

6. Нажмите на кнопку **Создать**.

TAP-сервис отобразится в таблице. Вы можете выполнить одно из следующих действий с TAP-сервисом, нажав на кнопку **Управление** рядом с ним и выбрав соответствующее значение в раскрывающемся списке:

- Изменить параметры TAP-сервиса, выбрав **Изменить**.

- Удалить TAP-сервис, выбрав **Удалить**. При необходимости удалить добавленные в сервис сервисные интерфейсы в окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

- Просмотреть статистику работы TAP-сервиса, выбрав **Статистика**.

Планировщик задач

Kaspersky SD-WAN поддерживает отложенный запуск задач с помощью планировщика. Обратите внимание, что для отложенного запуска задач на конкретных устройствах CPE их можно сгруппировать с помощью тегов.

На данный момент вы можете настроить отложенный запуск следующих типов задач (со временем этот список будет пополняться):

- Запуск скриптов на устройствах CPE – вам нужно предварительно добавить скрипты, которые вы хотите запустить, в шаблоне CPE.

- Обновление прошивок на устройствах CPE – вам нужно предварительно добавить прошивку, которую вы хотите установить, в веб-интерфейс оркестратора.

Когда вы назначаете отложенное выполнение задачи на определенное время, Kaspersky SD-WAN использует часовой пояс хоста оркестратора. Например, если вы запланировали запуск скрипта на устройстве CPE на 14:00, даже если оно находится в другом часовом поясе, скрипт будет запущен в соответствии с часовым поясом хоста оркестратора.

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 добавления.

- 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.

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**.

Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

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.

  Инструмент управления, мониторинга и диагностики сети SD-WAN, также отвечающий за виртуализацию сетевых функций (англ. Network Function Virtualization, NFV). Для управления оркестратором используется графический веб-интерфейс.

- **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 открыть страницу настройки кластера, чтобы изменить свойства контроллера. Вы не можете изменять свойства контроллера SD-WAN на странице настройки одного 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 разделе со списком свойств контроллера выберите вкладку **Изменяемые параметры**.
2. При необходимости сбросьте все свойства до значений по умолчанию, выполнив следующие действия:

a. Над списком свойств нажмите на кнопку настройки и в раскрывающемся списке выберите **Сбросить все параметры до значений по умолчанию**.

b. В окне подтверждения нажмите на кнопку **Сбросить**.

3. При необходимости сбросьте отдельное свойство до значения по умолчанию, выполнив следующие действия:

a. Нажмите на кнопку **Управление** рядом со свойством и в раскрывающемся списке выберите **Сбросить параметр до значения по умолчанию**.

b. В окне подтверждения нажмите на кнопку **Сбросить**.

4. При необходимости измените значение свойства, выполнив следующие действия:

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**.

Для отмены изменения свойств контроллера вам нужно удалить запланированные значения. Это действие применимо только к свойствам с методом изменения Reload.

Чтобы удалить запланированные значения свойств контроллера:

1. В разделе со списком свойств контроллера выберите вкладку **Изменяемые параметры**.

2. При необходимости удалите запланированные значения всех свойств, выполнив следующие действия:

a. Над списком свойств нажмите на кнопку настройки и в раскрывающемся списке выберите **Удалить все запланированные значения**.

b. В окне подтверждения нажмите на кнопку **Удалить**.

3. При необходимости удалите запланированное значение отдельного свойства, выполнив следующие действия:

a. Нажмите на кнопку **Управление** рядом со свойством и в раскрывающемся списке выберите **Удалить запланированное значение**.

b. В окне подтверждения нажмите на кнопку **Удалить**.

Запланированные значения свойств удалятся из базы данных контроллера SD-WAN и перестанут отображаться в столбце **Планируемое значение**.

Перезагрузка контроллера SD-WAN

Вам нужно перезагрузить контроллер SD-WAN, чтобы изменения свойств с методом изменения Reload вступили в силу. Если контроллер развернут в виде VNF для его перезагрузки требуется перезагрузить соответствующую VNF.

Чтобы перезагрузить контроллер SD-WAN:

1. На странице настройки сетевых сервисов в панели **Объекты** выберите вкладку **VNF**.
2. Нажмите на VNF, которая используется для работы контроллера SD-WAN.

   В нижней части страницы откроется область настройки VNF с выбранной по умолчанию вкладкой **Параметры развёртки**. Вы можете нажать на кнопку развертывания , чтобы развернуть область настройки VNF на всю страницу.
3. Нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Управление питанием → Программная перезагрузка VNF**.
4. В окне подтверждения нажмите на кнопку **Применить**.

На странице настройки свойств контроллера SD-WAN, на вкладке **Изменяемые параметры** планируемые значения свойств станут текущими и отобразятся в столбце **Текущее значение**. При этом все значения из столбца **Планируемое значение** будут удалены.

Просмотр информации об узлах контроллера SD-WAN

В дополнительном меню настройки веб-интерфейса отображаются все узлы контроллера SD-WAN – основной и второстепенные (если используются). Вы можете просматривать статистику работы каждого узла, а также список их свойств с указанными значениями.

Чтобы просмотреть информацию об узлах контроллера SD-WAN:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Узлы контроллера**.
2. Для просмотра статистики работы узла нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Статистика**.
3. Для просмотра свойств узла нажмите на кнопку **Управление** и в раскрывающемся списке выберите **Параметры 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, туннель между двумя устройствами CPE можно выбрать и настроить. Например, через топологию экземпляра SD-WAN вы можете указать стоимость туннеля и включить его мониторинг.

Чтобы просмотреть топологию развернутого экземпляра SD-WAN:

1. В дополнительном меню настройки веб-интерфейса перейдите в раздел **Топология**.
2. При необходимости установите следующие флажки:

   - **Загруженность каналов** – показать загруженность отображенных туннелей.

     Уровень загруженности туннеля соответствует следующим цветам:

     - Зеленый – малая загруженность туннеля.

- Желтый – средняя загруженность туннеля.
- Красный – высокая загруженность туннеля.

- **Сегменты** – выбрать два устройства CPE в раскрывающемся списке **Выберите два коммутатора**, после чего отобразить все туннели, используемые в выбранном сегменте.
- **Внутриполосное управление** – 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.

- **Имя** – отобразить имена устройств CPE, используемых в топологии.
- **IP-адрес** – 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.

Глоссарий

Customer Premise Equipment (CPE)

Телекоммуникационное оборудование, включающее в себя виртуальные машины, которое обеспечивает передачу трафика в рамках сети SD-WAN. Трафик может передаваться в ЦОД для предоставления сетевых функций, например работы протоколов маршрутизации, предотвращения вторжений или антивируса.

Physical Network Function (PNF)

Заранее развернутая сетевая функция, которая 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)

Менеджер, обеспечивающий управление и мониторинг вычислительных и сетевых ресурсов, а также ресурсов хранения в виртуальной инфраструктуре. С его помощью VNF взаимодействуют со всеми этими ресурсами.

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)

Инструмент конфигурации VNF, развернутых оркестратором.

Контроллер SD-WAN

Центральный компонент сети SD-WAN, обеспечивающий управление наложенной сетью, включая построение актуальной топологии, настройку устройств CPE и создание транспортных сервисов.

Оркестратор

Инструмент управления, мониторинга и диагностики сети SD-WAN, также отвечающий за виртуализацию сетевых функций (англ. Network Function Virtualization, NFV). Для управления оркестратором используется графический веб-интерфейс.

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

Осуществляет передачу пакетов трафика. Плоскость передачи данных образуют устройства CPE.

Плоскость управления сетью

Контролирует передачу пакетов трафика по сети через устройства CPE. В плоскость управления трафиком входят оркестратор и контроллер SD-WAN.

Тенант

Клиент вашей организации, которому выделяется логический набор сетевых и/или вычислительных ресурсов, для построения сети SD-WAN.

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.

Ansible, CentOS, Red Hat — товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

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.

Kraftway – зарегистрированный товарный знак ЗАО "Крафтвэй корпорэйшн ПЛС".

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft Edge является товарным знаком 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.