kaspersky

Kaspersky SD-WAN

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 контролирует передачу пакетов трафика по сети через **устройства Customer Premise Equipment** (далее устройства CPE, устройства), установленные на клиентских площадках. 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.

В сетях, построенных с применением технологии SDN, плоскость управления сетью включает в себя **контроллер SD-WAN** и **оркестратор**. Обратите внимание, что управление также может осуществляться через API.

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.

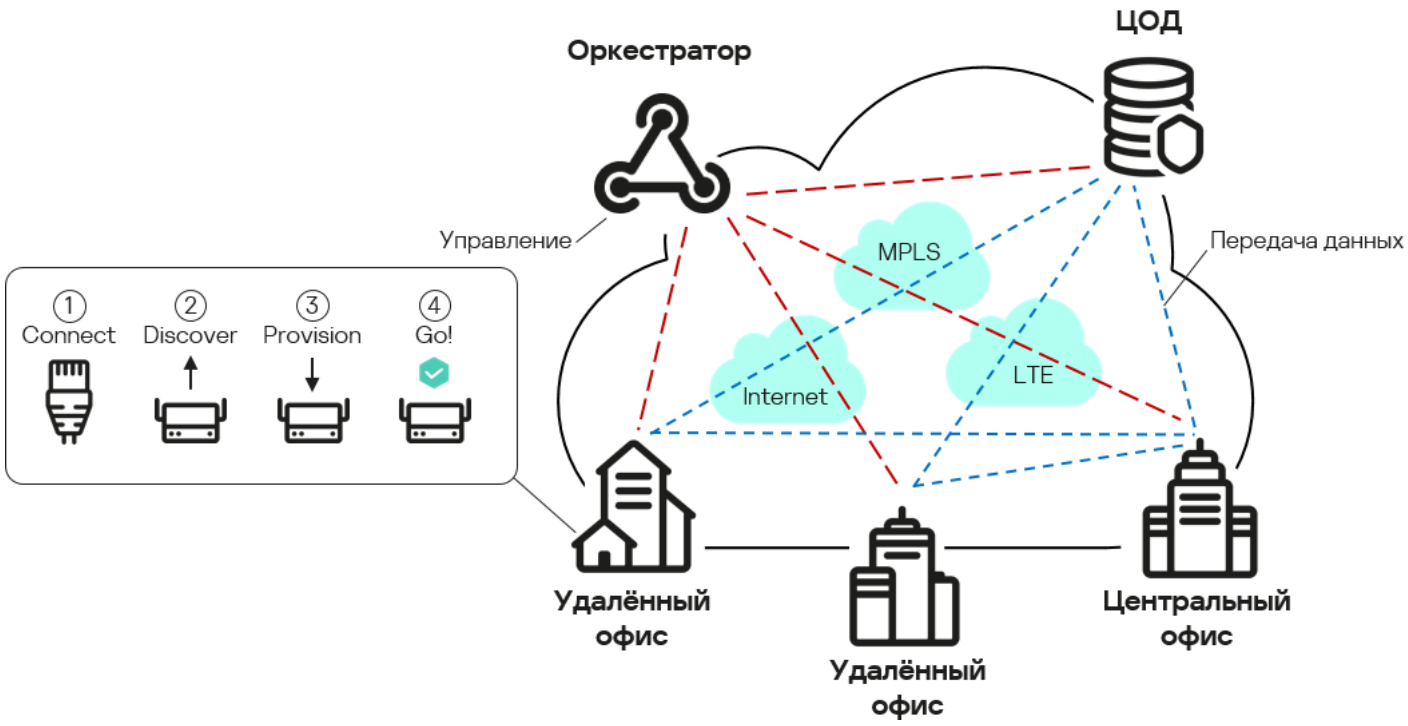


Схема сети SD-WAN

При развертывании Kaspersky SD-WAN вы можете использовать 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**. Используемый программный модуль 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. Используемый программный модуль 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. Если требуется, 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 машины 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:

- Debian версии 8.1 и выше.
- Ubuntu версии 14.04 и выше.
- CentOS версии 7.1 и выше.
- Red Hat версии 7.1 и выше.

- SUSE версии 12.4 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

Помимо заявленных "Лабораторией Касперского" устройств CPE решение также может поддерживать сторонние устройства. Для уточнения возможности использования стороннего устройства просьба обратиться в техническую поддержку. Вне зависимости от модели устройства к нему предъявляются следующие технические требования:

- стандартная архитектура процессора x86 или Arm;
- не менее двух ядер процессора;
- не менее 128 МБ оперативной памяти;
- не менее одного LAN-интерфейса;
- не менее одного WAN-интерфейса.

В таблице ниже представлены модели устройств CPE, которые были успешно протестированы на совместимость с решением специалистами "Лаборатории Касперского". В ходе тестирования проверялась работоспособность устройства при предоставлении услуги L3 WAN.

Протестированные модели устройств CPE (услуга L3 WAN)

Модель	Процессор	Оперативная память	Жесткий диск
Булат BM10-2xLTE-HP	MediaTek MT7621, 2 ядра, 4 потока	256 МБ	16 МБ
Kraftway Рубеж-H	Intel Celeron CPU J3455, частота ядра 1.50 ГГц	8 ГБ	128 ГБ
Булат BM1300	Intel Atom CPU C3758, частота ядра 2.20 ГГц	8 ГБ	240 ГБ
Kraftway Рубеж-C	Intel Xeon D-1559, 12 ядер	16 ГБ	128 ГБ
Kraftway Рубеж-T	2 процессора Intel Xeon Gold 5318Y (Ice Lake-SP), 24 ядра, частота ядер 2.1 ГГц	64 ГБ	256 ГБ

Специалисты "Лаборатории Касперского" также 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)
Булат BM10-2xLTE-HP	IMIX (417)	30
	Large (1300)	115
Kraftway Рубеж-H	IMIX (417)	165
	Large (1300)	241
Булат BM1300	IMIX (417)	378
	Large (1300)	604
Kraftway Рубеж-C	IMIX (417)	805
	Large (1300)	1150
Kraftway Рубеж-T	IMIX (417)	2875
	Large (1300)	5750

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.
- Следующие устройства были протестированы на совместимость с решением:
  - Bulat BM10-2xLTE-HP.
  - Kraftway Rubej-N.
  - Kraftway Rubej-S.
  - Kraftway Rubej -2C.
  - Kraftway Rubej-T.

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.

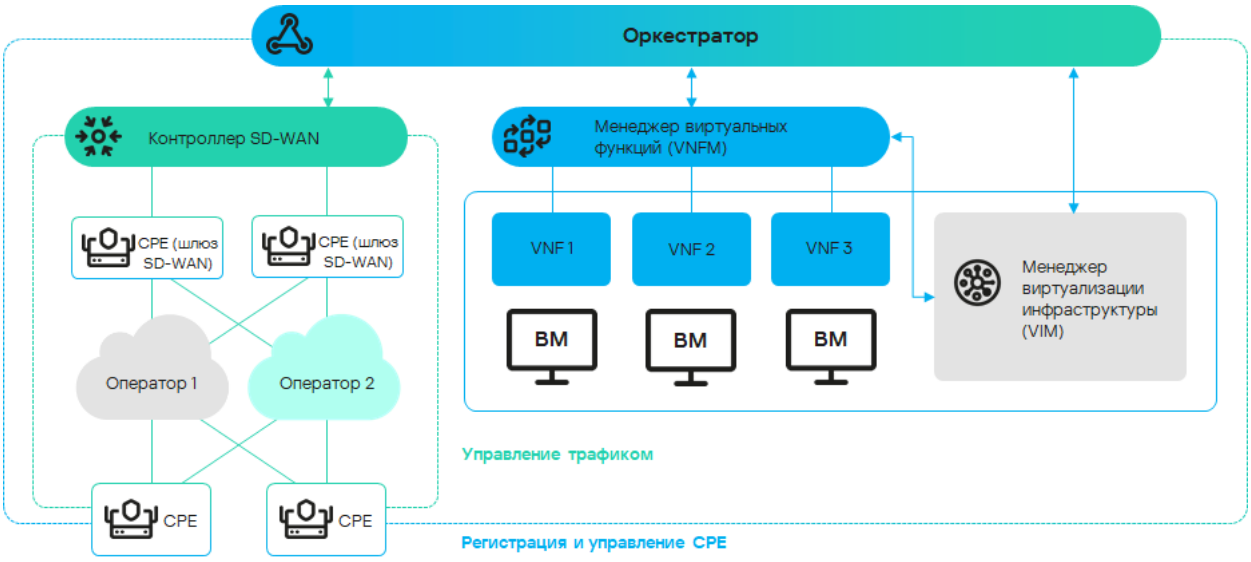
При создании и регистрации устройств CPE для отдельных клиентских тенантов, вы можете назначать эти устройства одному транспортному тенанту, если хотите построить сеть SD-WAN с использованием ограниченного количества устройств. В этом случае тенанты делят между собой контроллер SD-WAN, но имеют отдельные 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 с образом виртуальной машины для контроллера SD-WAN. Файл образа имеет формат QCOW2. Эта папка не входит в состав пакета PNF.
- VNF- или PNF-дескриптор. Файл с именем vnfd или pnfd, который описывает параметры сетевой функции и имеет формат XML или YAML.
- Папка со скриптами 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

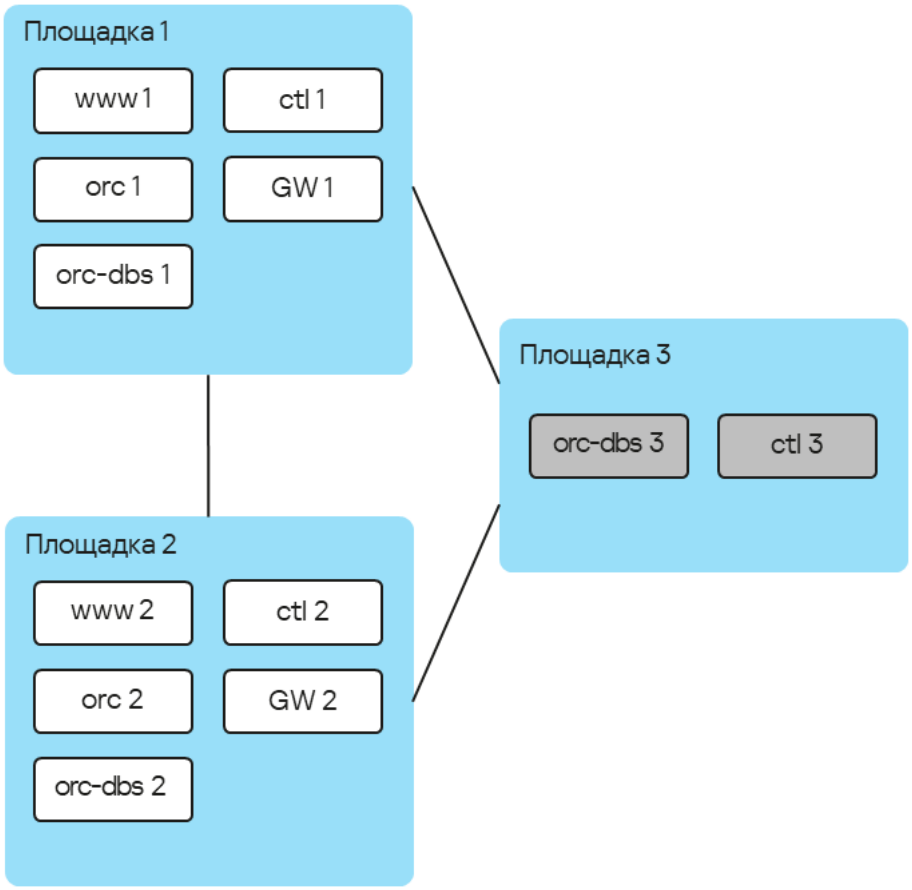
Компонент	Схема резервирования	Используемый протокол
Оркестратор	N+1	REST
Веб-интерфейс оркестратора	N+1	REST
База данных оркестратора	2N+1	MONGODB
Контроллер SD-WAN и его база данных	2N+1	OPENFLOW (TLS)
Шлюз SD-WAN	N+1	GENEVE

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.

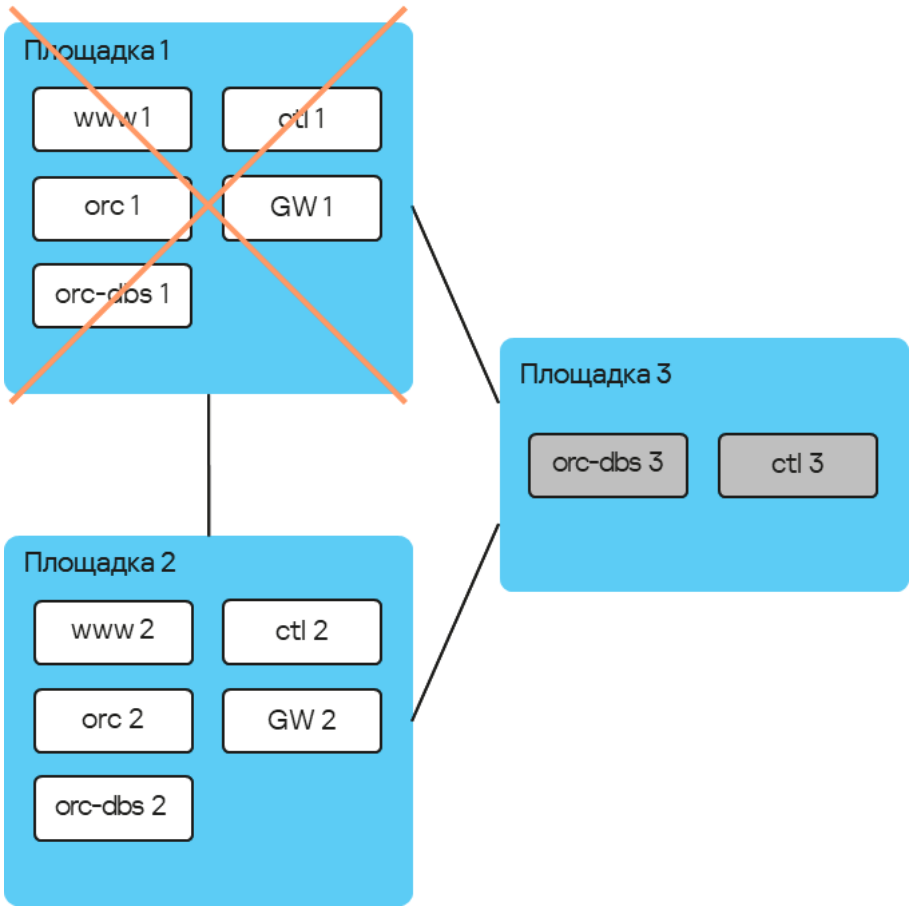


Размещение компонентов решения в географически разнесенных ЦОД

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.

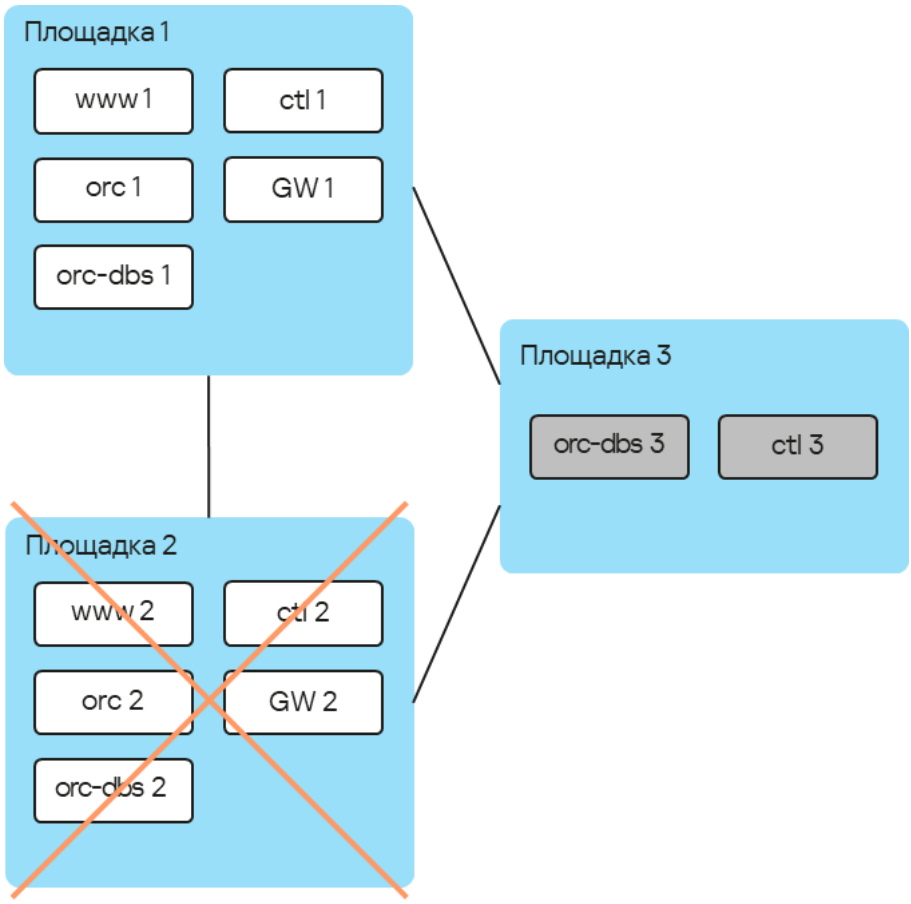


Авария на площадке 1

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.

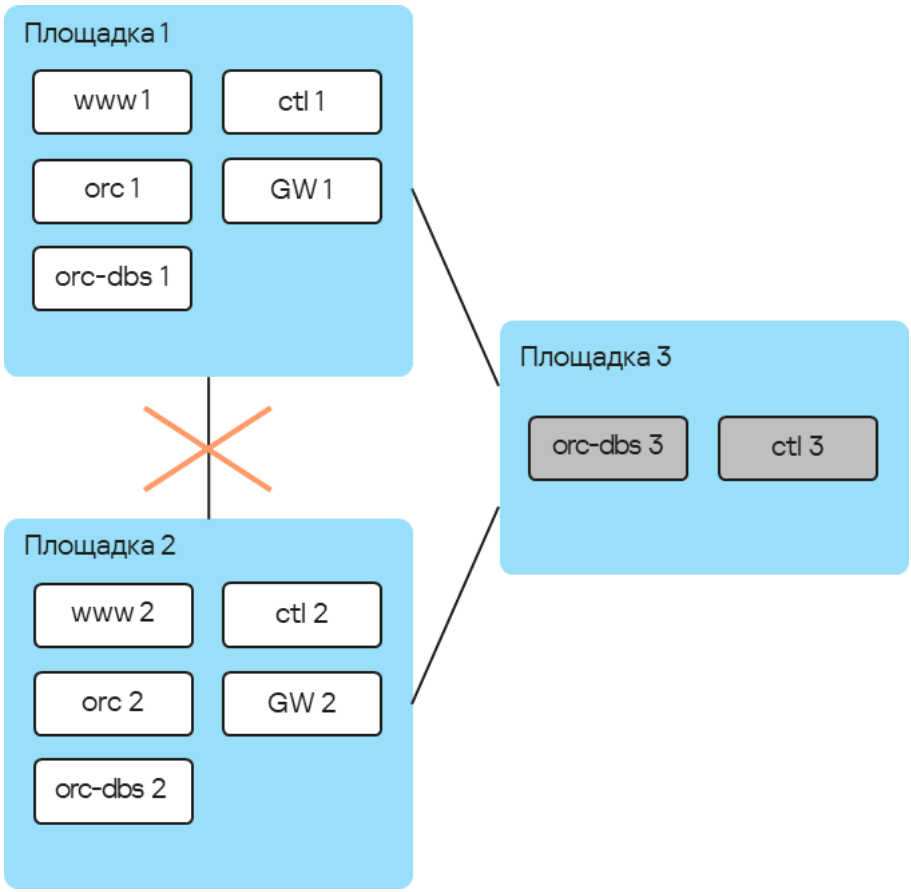


Авария на площадке 2

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.

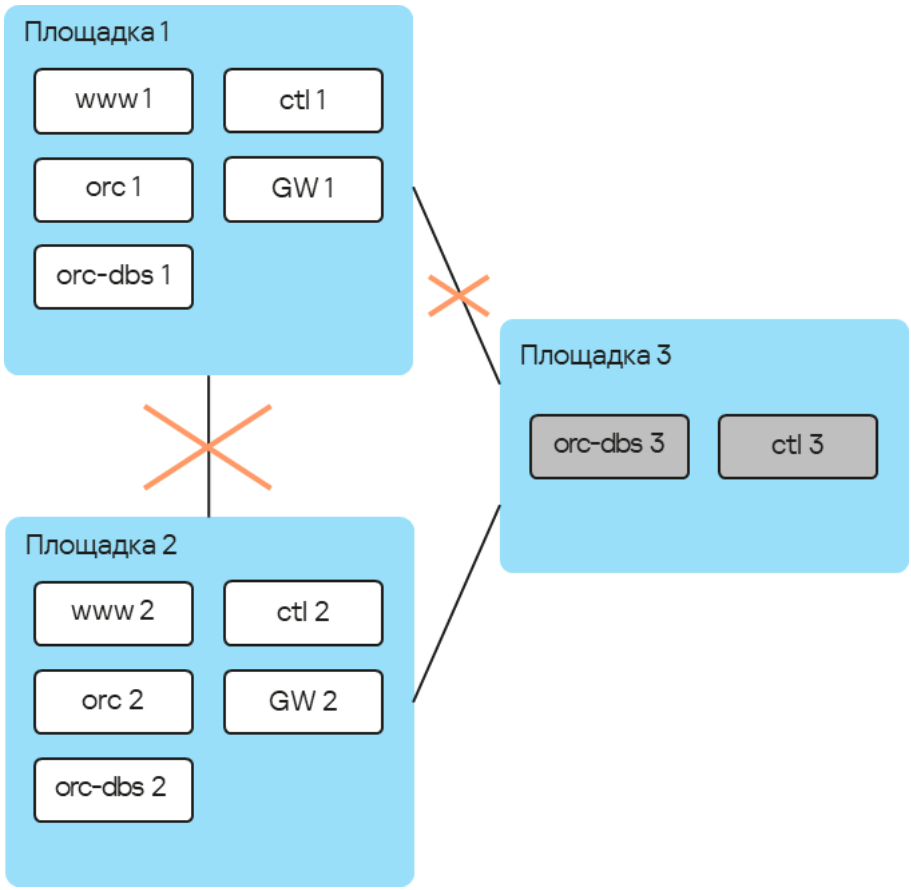


Авария на соединении между площадками 1 и 2

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- 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 имеет три режима:

- 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.

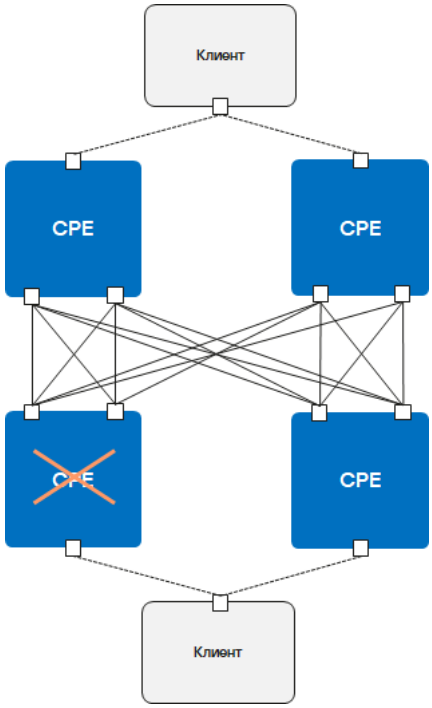
Режим Active/Standby

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.

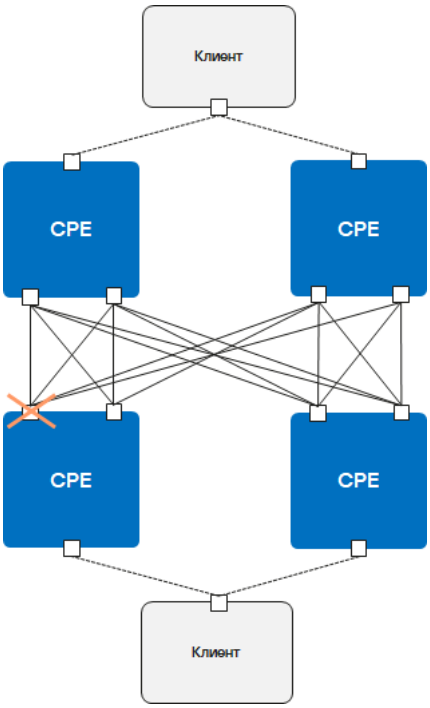
Вы можете настроить резервирование на уровне транспортных сервисов. В этом случае при создании транспортного сервиса указываются резервные сервисные интерфейсы (англ. reserve SI) на выбранном устройстве CPE или на другом устройстве. Мы рекомендуем создавать основной и резервный сервисные интерфейсы на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

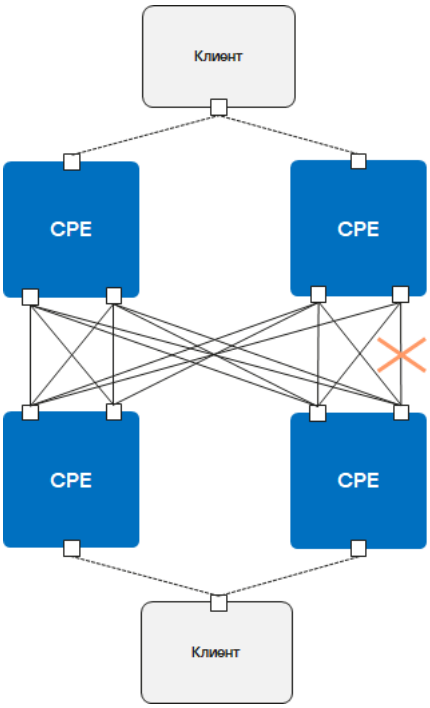
- Выход из строя одного из устройств CPE.



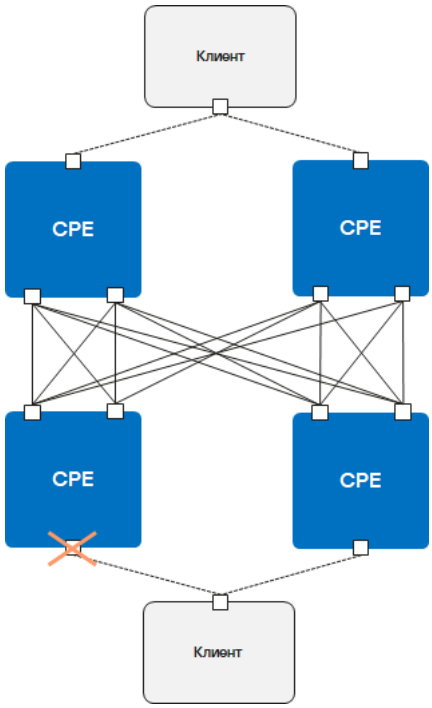
- Выход из строя WAN-интерфейса одного из устройств CPE.



- Выход из строя связности между двумя устройствами CPE.



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



Обеспечение безопасности

Безопасность в Kaspersky SD-WAN обеспечивается в плоскостях **передачи данных**, **управления сетью** и оркестрации. Степень безопасности всего решения определяется степенью безопасности каждой из этих плоскостей, а также 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 Active Directory, которую вы добавляете с помощью сервера LDAP и, если требуется, 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 будет находиться устройство CPE после успешной регистрации – *активировано* или *не активировано*. Не активированное устройство CPE требуется активировать вручную, убедившись, что оно установлено на нужной 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:

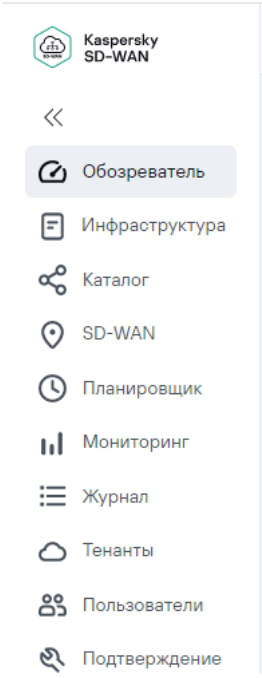
Устройства CPE с дополнительной поддержкой развертывания виртуальных сетевых функций. Обратите внимание, что устройство должно иметь достаточно аппаратных ресурсов для того, чтобы не задействовать ЦОД или облако во время предоставления VNF.

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.



Навигационная панель

Навигационная панель содержит следующие разделы:

- **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** ( ). В этом разделе вы можете настраивать вашу сетевую инфраструктуру, например добавлять домены, 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** ( ). В этом разделе вы можете настраивать устройства CPE, экземпляры SD-WAN и UNI, а также управлять прошивками и сертификатами устройств.
- **Планировщик** ( ). В этом разделе вы можете настраивать отложенный запуск задач и назначать их на определенное время.
- **Журнал** ( ). В этом разделе вы можете просматривать журналы работы различных компонентов решения. Например, здесь отображаются внесенные другими пользователями изменения в параметры устройств CPE.
- **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** ( ). 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, создавать группы Active Directory и настраивать доменную аутентификацию.
- **Подтверждение** ( ). В этом разделе вы можете управлять запросами на подтверждение. Пользователи, учетная запись которых имеет статус *read-only*, отправляют запросы на подтверждение, чтобы изменять параметры компонентов 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 ».

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**.

Параметры подключения к Zabbix

Чтобы перейти в раздел настройки подключения к Zabbix,

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

Параметры сетевых сервисов

Чтобы перейти в раздел настройки сетевых сервисов,

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

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 вы хотите настроить.

Параметры устройства CPE

Чтобы открыть область настройки устройства CPE:

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

Управление тенантами

Чтобы перейти в раздел управления тенантами,

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

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 вы хотите настроить.

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 вы хотите настроить.

Дополнительное меню настройки решения

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

Чтобы перейти в дополнительное меню настройки решения:

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**.

Параметры контроллера SD-WAN

Чтобы перейти к списку параметров 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 параметров контроллера SD-WAN, как изменяемых (Reload и Runtime), так и неизменяемых (Read-only).
3. Если необходимо отобразить только изменяемые параметры, выберите вкладку **Изменяемые параметры**.

Над списком параметров находится поле поиска (), с его помощью вы можете найти нужные параметры по методу изменения, имени параметра, его значению 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**.

Переключение между светлой и темной темой веб-интерфейса оркестратора

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**.

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**. 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 добавленный домен.

Чтобы создать домен:

1. На странице управления инфраструктурой решения нажмите на кнопку **+ Домен**.
2. В открывшемся окне укажите параметры домена:
   - **Имя**. Диапазон значений: от 1 до 50 символов.
   - **Описание**. Максимальная длина: 100 символов.
3. Нажмите на кнопку **Сохранить**.

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

Добавление центра обработки данных

Центральные компоненты Kaspersky SD-WAN, за исключением **устройств CPE**, размещаются в центрах обработки данных. При добавлении ЦОД 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 укажите параметры центра обработки данных:
   - **Имя**. Диапазон значений: от 1 до 20 символов.
   - **Описание**.
   - **Домен**. Домен, в который требуется добавить центр обработки данных.
   - **VNFM URL**. Если требуется, вы можете нажать на кнопку **Проверить соединение**, чтобы убедиться в доступности VNFM.

- **Адрес**. Почтовый адрес ЦОД.

3. Нажмите на кнопку **Сохранить**.

Центр обработки данных отобразится в панели **Ресурсы**.

Создание диапазона IP-адресов

Каждому компоненту Kaspersky SD-WAN автоматически присваивается IP-адрес для внутреннего управления (англ. in-band management). Присвоение IP-адреса происходит из определенного диапазона IP-адресов.

Вам нужно создать как минимум один диапазон IP-адресов для каждого центра обработки данных, используемого в вашей организации. При создании диапазона вы можете указать IP-адреса DNS-серверов и статические маршруты, чтобы передавать их компонентам решения вместе с IP-адресами.

Чтобы создать диапазон IP-адресов:

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

2. В открывшемся окне укажите параметры подсети:

   - **Домен** и **ЦОД**. Параметры, позволяющие выбрать центр обработки данных, для которого требуется создать диапазон IP-адресов.

   - **Имя**.

   - **Версия IP**.

     Доступные значения:

     - **IPv4**.

     - **IPv6**.

   - **CIDR**. Подсеть и маска для диапазона IP-адресов.

   - **Шлюз**. IP-адрес шлюза.

   - **Диапазон IP**. Блок для создания диапазонов IP-адресов. Для создания диапазона нажмите на кнопку **+ Добавить** и укажите его в отобразившихся полях.

   - **DNS**. Блок для указания IP-адресов DNS-серверов, используемых в подсети. Для добавления адреса нажмите на кнопку **+ Добавить** и введите его в отобразившемся поле. Компоненты решения получают IP-адрес DNS-сервера вместе с IP-адресами из диапазона.

   - **Статические маршруты**. Блок для создания статических маршрутов в подсети. Для создания статического маршрута нажмите на кнопку **+ Добавить** и введите его в отобразившемся поле. Компоненты решения получают статический маршрут вместе с IP-адресами из диапазона.

3. Нажмите на кнопку **Сохранить**.

Диапазон IP-адресов отобразится на вкладке **IPAM**.

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 укажите параметры VIM:
   - **Домен** и **ЦОД**. Параметры, позволяющие выбрать центр обработки данных, для которого требуется добавить VIM.
   - **Имя**.
   - **IP**. IP-адрес или доменное имя для подключения оркестратора к VIM.
   - **Порт**. Номер порта для подключения оркестратора к VIM.
   - **Протокол**. Протокол для подключения оркестратора к VIM.

     Доступные значения:

     - **http**;
     - **https**.
   - **Имя пользователя** Имя пользователя учетной записи OpenStack с правами администратора для авторизации в VIM.
   - **Пароль**. Пароль учетной записи OpenStack с правами администратора для авторизации в VIM.
   - **Проект администратора**. Имя проекта администратора OpenStack для авторизации в VIM.
   - **Домен**. Имя OpenStack-домена.
   - **За NAT**. Параметр, позволяющий определить, находится ли VIM за NAT (Network Address Translation).

     Доступные значения:

     - **Включено**. VIM находится за NAT.
     - **Выключено**. VIM не находится за NAT.

- **Переподписка ЦП**. Коэффициент переподписки при предоставлении виртуальных процессорных ядер.
- **Переподписка ОЗУ**. Коэффициент переподписки оперативной памяти.
- **Переподписка диска**. Коэффициент переподписки дискового пространства.
- **Количество потоков**. Максимальное количество потоков при взаимодействии оркестратора с VIM.
- **Кластер SDN**. SDN-кластер, к которому подключен OpenStack. Если OpenStack не подключен к SDN-кластеру, выберите **None**.
- **Диапазон VLAN ID**. Максимальное количество VLAN для OpenStack. Диапазон значений: от 0 до 4094.
- **Имя physnet для SR-IOV**. Имя physnet для сетей с типом подключения SR-IOV. Этот тип подключения используется с сегментацией VLAN.
- **Физическая VLAN-сеть**. Имя physnet для VLAN-сетей.

3. Если в раскрывающемся списке **Кластер SDN** вы выбрали SDN-кластер, укажите параметры подключения к кластеру SDN:
   - **OpenStack-сеть**. Имя сети OpenStack, к которой подключен VIM.
   - **Группа интерфейсов**. Группа интерфейсов, через которую все узлы OpenStack подключены к SDN-кластеру.
   - **Управляющая группа**. Группа интерфейсов, через которую управляющие узлы OpenStack подключены к SDN-кластеру.
   - **Вычислительная группа**. Группа интерфейсов, через которую вычислительные узлы OpenStack подключены к SDN-кластеру.
4. Если в раскрывающемся списке **Кластер SDN** вы выбрали **None**, укажите следующие параметры:
   - **Имя physnet для FLAT**. Имя physnet для сетей с сегментацией FLAT.
   - **Имя physnet для VXLAN**. Имя physnet для сетей с сегментацией VXLAN.
   - **Сегментация управляющей сети**. Тип сегментации используемый управляющей сетью.

     Доступные значения:
     - **VLAN**.
     - **VXLAN**.
   - **ID управляющего сегмента**. ID сегмента управляющей сети. Диапазон значений: от 0 до 16 000 000.
   - **Port security**. Параметр, позволяющий включить или выключить функцию Port security.

     Доступные значения:
     - **Включено**.
     - **Выключено**.
   - **Разрешить CIDR**. Адрес разрешенной подсети для сети управления.

5. Нажмите на кнопку **Сохранить**.

VIM отобразится на вкладке **Вычислительные ресурсы**.

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 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.

Загрузка пакета VNF или PNF в оркестратор

Контроллер SD-WAN может быть развернут в виде **VNF** или **PNF**. В зависимости от выбранной схемы развертывания специалисты "Лаборатории Касперского" предоставляют вам один из следующих пакетов:

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).

- **Пакет VNF**.

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

- **Пакет PNF**.

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

Полученный архив требуется загрузить в веб-интерфейс оркестратора.

Чтобы загрузить пакет VNF или PNF в оркестратор:

1. На странице настройки сетевых сервисов нажмите на кнопку **+ VNF** или **+ PNF**.

2. Выберите файл пакета PNF или VNF, который вы хотите загрузить.

Загруженная сетевая функция отобразится в панели **Каталог** на вкладке **VNF** или **PNF**.

Создание шаблона сетевого сервиса SD-WAN

Вы можете поместить VNF или PNF контроллера SD-WAN в шаблон сетевого сервиса, чтобы позже развернуть отдельный экземпляр SD-WAN для тенанта. Перед выполнением этой инструкции требуется загрузить пакет VNF или PNF в оркестратор.

Чтобы создать шаблон сетевого сервиса SD-WAN:

1. На странице настройки сетевых сервисов нажмите на кнопку **+ Шаблон**.
2. В панели **Каталог** слева выберите одну из следующих вкладок:
   - **VNF**. Для развертывания контроллера SD-WAN в виде VNF.
   - **PNF**. Для развертывания контроллера SD-WAN в виде PNF.
3. Перетащите сетевую функцию контроллера в графический конструктор.
4. Если требуется, добавьте другие компоненты в топологию сетевого сервиса SD-WAN.
5. В поле **Имя** введите имя шаблона сетевого сервиса SD-WAN.
6. Вверху справа нажмите на кнопку **Сохранить**.

Шаблон сетевого сервиса SD-WAN отобразится в панели **Каталог** на вкладке **Шаблоны**.

Создание тенанта

Вы можете создавать тенантов для назначения определенного логического набора сетевых и/или вычислительных ресурсов клиентам вашей организации.

Чтобы создать тенанта,

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 ＋.
- Если вы создаете последующих тенантов, нажмите на кнопку **+ Тенант**, затем в поле **Имя** введите имя тенанта и нажмите на кнопку создания ＋.

Тенант отобразится в блоке **Тенанты**.

Развертывание сетевого сервиса SD-WAN для тенанта

Вы можете развернуть сетевой сервис с контроллером SD-WAN для тенанта, чтобы создать для него отдельный экземпляр SD-WAN. Перед выполнением этой инструкции требуется создать шаблон сетевого сервиса SD-WAN.

Чтобы развернуть сетевой сервис SD-WAN для тенанта

1. В разделе управления тенантами в блоке **Тенанты** нажмите на тенанта, для которого требуется развернуть сетевой сервис SD-WAN.
2. Внизу слева нажмите на кнопку **Подключиться как тенант**.

   Вы будете авторизованы в веб-интерфейсе тенанта как администратор и по умолчанию отобразится раздел **Каталог**.
3. В панели **Сетевые сервисы** нажмите на кнопку **+ Добавить сервис**.
4. В отобразившейся панели **Каталог** выберите вкладку **Шаблоны**.
5. Перетащите шаблон сетевого сервиса SD-WAN мышью в графический конструктор.

   Топология, которую вы указали при создании шаблона сетевого сервиса SD-WAN, отобразится в графическом конструкторе.
6. В поле **Имя** введите имя сетевого сервиса SD-WAN.
7. Вверху справа нажмите на кнопку **Развернуть**.

Начнется развертывание сетевого сервиса SD-WAN. Вы можете прервать развертывание, нажав на кнопку **Прервать развертывание**.

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 **Журнал**.
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**. Если требуется, нажмите на идентификатор ID запроса на обслуживание, чтобы открыть пошаговый журнал его выполнения с подробной информацией о каждом шаге. 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 (статус *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 следующих разделах веб-интерфейса оркестратора:

- **Устройства CPE**. Запросы на обслуживание отдельного устройства.
- **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. В области настройки устройства CPE или экземпляра SD-WAN выберите вкладку **Запросы на обслуживание**.

Запросы на обслуживание отобразятся в таблице.

2. Если требуется, выполните следующие действия:

   - Нажмите на идентификатор ID запроса на обслуживание, чтобы открыть пошаговый журнал его выполнения с подробной информацией о каждом шаге. Журнал содержит информацию о шагах, на которых произошли ошибки, а также подробное описание самих ошибок.

   - Нажмите на кнопку **Удалить**, рядом с требуемым запросом на обслуживание.

   - 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 устройства CPE.

Работа с экземплярами SD-WAN

Экземпляром SD-WAN (англ. SD-WAN instance) является развернутое для одного **тенанта** решение Kaspersky SD-WAN. 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 кластера 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 изменить имя в области настройки шаблона экземпляра SD-WAN в поле **Имя**.

Действия с шаблоном экземпляра SD-WAN

После создания шаблона экземпляра SD-WAN вы можете выполнять с ним действия, которые отображаются в соответствующем блоке.

Чтобы выполнить требуемое действие с шаблоном экземпляра SD-WAN,

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

- **Удалить**.
- **Назначить шаблоном по умолчанию**. Шаблон по умолчанию используется при развертывании экземпляра SD-WAN для тенантов, которые не добавлены ни в один из шаблонов.

Добавление тенанта в шаблон экземпляра SD-WAN

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.
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. На данный момент Kaspersky SD-WAN поддерживает одну транспортную стратегию B4N 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**. При удалении экземпляра SD-WAN удаляются 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**. Кнопка, позволяющая 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 будет осуществлять 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.

Переход в дополнительное меню настройки решения через экземпляр SD-WAN

Чтобы перейти в дополнительное меню настройки решения через экземпляр SD-WAN,

вверху области настройки экземпляра SD-WAN нажмите на кнопку **Управление контроллером**.

Переход на страницу настройки сетевых сервисов через экземпляр SD-WAN

Чтобы перейти на страницу настройки сетевых сервисов через экземпляр SD-WAN,

вверху области настройки экземпляра SD-WAN нажмите на кнопку **Управление сетевым сервисом SD-WAN**.

В новой вкладке браузера откроется веб-интерфейс экземпляра SD-WAN. При этом вы будете автоматически авторизованы как администратор тенанта и перейдете в раздел **Каталог**.

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.

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 вы хотите добавить в пул.

7. Нажмите на кнопку **Добавить**.

   Экземпляр SD-WAN отобразится в таблице.

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.
- 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.

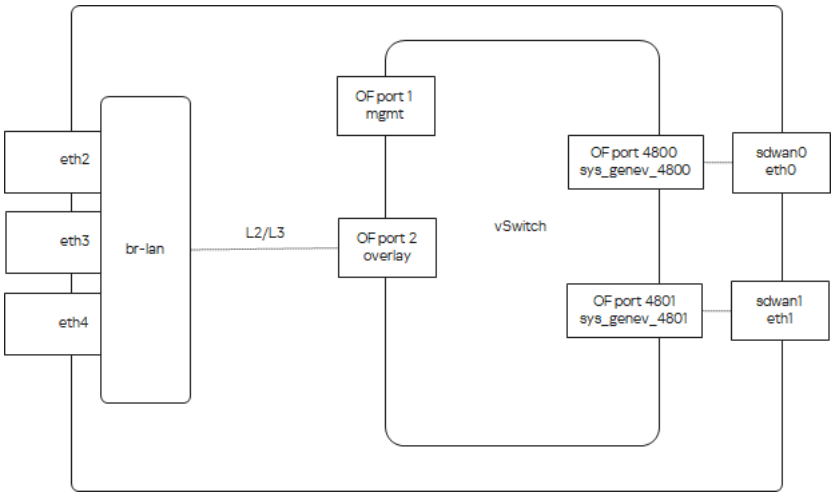
- 2 (ovs-lan). Обеспечивает подключение к Linux-мосту.

- 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). Вы можете установить программное обеспечение uCPE на 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.

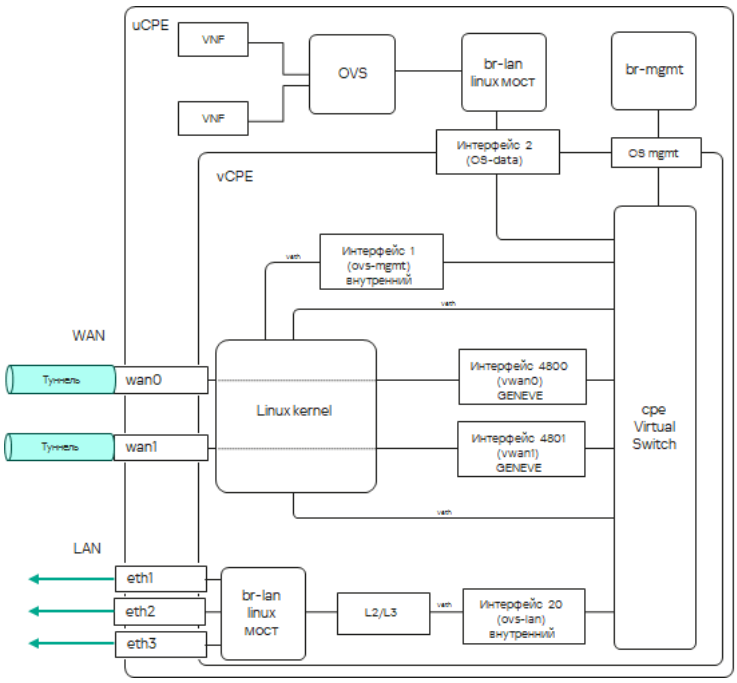
Вы можете создать сетевой сервис на устройстве uCPE, которое находится в состоянии *Отключено*. В этом случае оркестратор отслеживает доступность устройства uCPE и создает сетевой сервис в момент, когда VIM начинает отвечать на API-запросы.

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.



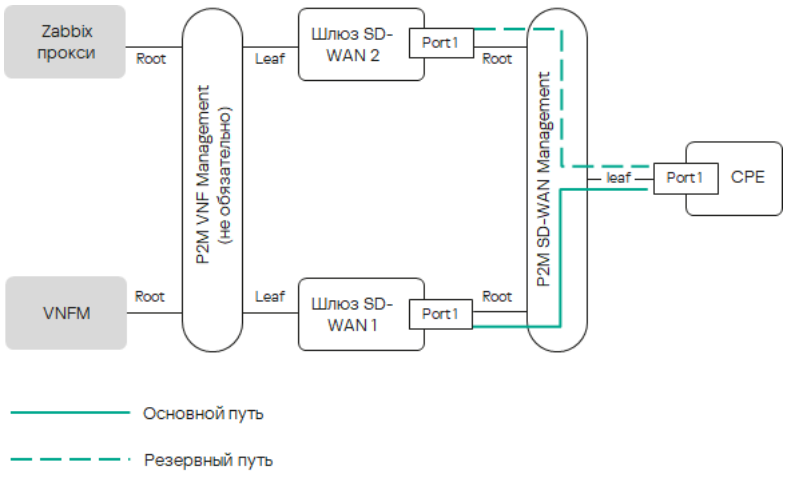
Логическая схема устройства uCPE

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 первую очередь (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.

Как правило, регистрация устройств CPE проходит по двум сценариям: 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. Если вы хотите провести дополнительную конфигурацию устройства CPE, вам нужно использовать URL-активацию.
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 полное имя домена (англ. Fully Qualified Domain Name, 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.

Чтобы автоматически настроить 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.

Кроме того, 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.
- *Не активировано* (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.

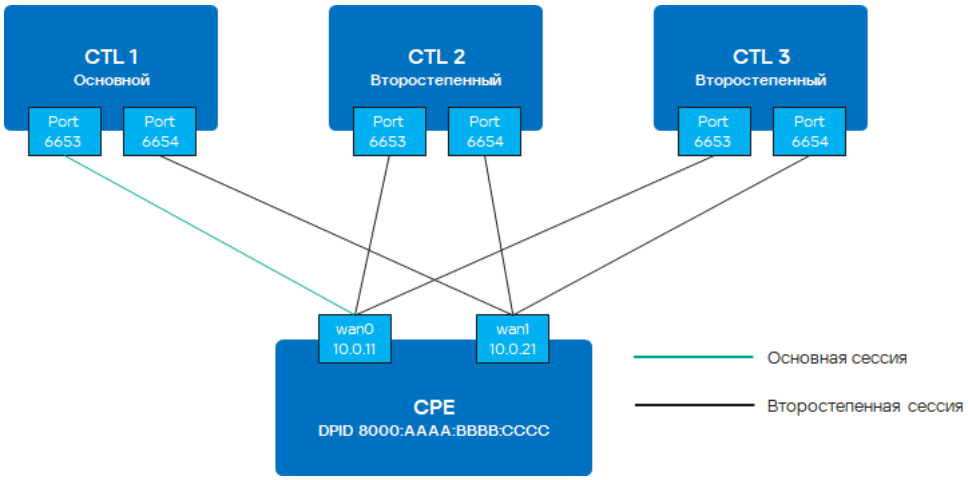
- *Не активировано* (в статусе *Зарегистрировано*). Устройству заблокирована передача трафика по туннелям, и оркестратор не отвечает на поступающие от него запросы.

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. Если требуется, 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 укажите параметры шаблона CPE:

- **Имя**.
- **Тип**.

  Доступные значения:

  - **CPE**. Шаблон **стандартного 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.

  - **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 вы можете настроить его, после чего применить к требуемым устройствам.

Действия с шаблоном CPE

После создания шаблона CPE, вы можете выполнять с ним действия, которые отображаются в соответствующем блоке.

Чтобы выполнить требуемое действие с шаблоном CPE,

в области настройки шаблона CPE в блоке **Действия** нажмите на одну из следующих кнопок:

- **Удалить**. Вы не можете удалить шаблон, который применен к устройствам CPE.
- **Импортировать**. Кнопка, позволяющая импортировать в шаблон CPE конфигурацию другого шаблона. Вы можете выбрать определенные вкладки шаблона, чтобы изменить указанные на них параметры в соответствии с импортируемой конфигурацией. Параметры, указанные на не выбранных вкладках, не изменяются. 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**. Кнопка, позволяющая экспортировать конфигурацию шаблона CPE. На ваше локальное устройство сохраняется 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.

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

Решение типовых задач с устройством CPE

После завершения работы с шаблоном CPE вы можете перейти к созданию и настройке отдельных устройств CPE. 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 следующих подразделах веб-интерфейса оркестратора:

- **Устройства CPE**.
- **Экземпляры SD-WAN**.

Чтобы создать устройство CPE:

1. Откройте окно создания устройства CPE одним из следующих способов:
   - 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. Укажите параметры устройства CPE:
   - **Имя**.
   - **DPID**.

- **Установить состояние**. Состояние устройства после регистрации.

  Доступные значения:

  - **Активировано**. Применить к устройству конфигурацию шаблона CPE. Активированное устройство можно подключать к транспортным сервисам и использовать для передачи трафика.
  - **Деактивировано**. Не применять к устройству конфигурацию шаблона CPE. Вы можете внести локальные изменения в конфигурацию устройства перед активацией.

- **Описание**.
- **Тенант**. Основной тенант. В качестве значения для этого параметра вы также можете указать пул экземпляров SD-WAN или отдельный экземпляр из пула.
- **Клиентский тенант**. Тенант организации вашего клиента.
- **Шаблон UNI**. Шаблон UNI, который требуется применить к устройству.
- **Шаблон CPE**. 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 подразделе **Экземпляры SD-WAN**, в новой вкладке браузера откроется веб-интерфейс экземпляра SD-WAN. Вы будете автоматически авторизованы как администратор тенанта.
- Если вы создали устройство в подразделе **Устройства CPE**, оно отобразится в этом подразделе.

Теперь вы можете настроить созданное устройство CPE, после чего использовать его для передачи трафика.

Действия с устройством CPE

После создания устройства CPE, вы можете выполнять с ним действия, которые отображаются в соответствующем блоке.

Чтобы выполнить требуемое действие с устройством CPE,

в области настройки устройства CPE в блоке **Действия** нажмите на одну из следующих кнопок:

- **Удалить**.
- **Указать адрес**.
- **Активировать** или **Деактивировать**. При активации устройства к нему применяется конфигурация шаблона CPE. Не активированное устройство невозможно использовать для передачи трафика.
- **Показать пароль**.

- **Получить URL активации**. Кнопка, позволяющая отобразить URL для активации устройства CPE.
- **Зарегистрировать** или **Отменить регистрацию**. Кнопки, позволяющие зарегистрировать устройство CPE или отменить его регистрацию. Кнопка **Зарегистрировать** отображается только для устройств, которые подключились к оркестратору и не были сопоставлены ни с одной из созданных записей.
- **Открыть SSH-консоль**. Кнопка, позволяющая подключиться к консоли устройства CPE по протоколу SSH. В новой вкладке веб-браузера откроется окно консоли.
- **Открыть веб-консоль**. Кнопка, позволяющая подключиться к веб-консоли устройства CPE. В новой вкладке веб-браузера откроется окно консоли и вам потребуется выполнить авторизацию.
- **Запустить скрипты**. Кнопка, позволяющая запустить все добавленные на устройстве CPE скрипты.
- **Перезагрузить**.
- **Выключить**. При выключении в оперативную систему устройства CPE отправляется команда `shutdown`.
- **Экспортировать параметры SD-WAN**. Кнопка, позволяющая экспортировать параметры подключения устройства CPE к сети SD-WAN, а также конфигурацию интерфейсов SD-WAN. На ваше локальное устройство сохранится файл в формате JSON с именем <Имя устройства>sdwan-config.
- **Экспортировать сетевые интерфейсы**. Кнопка, позволяющая экспортировать конфигурацию сетевых интерфейсов. 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 укажите параметры устройства CPE:
   - **Установить состояние**. Состояние устройства после регистрации.

     Доступные значения:

     - **Активировано**. Применить к устройству конфигурацию шаблона CPE. Активированное устройство можно подключать к транспортным сервисам и использовать для передачи трафика.
     - **Деактивировано**. Не применять к устройству конфигурацию шаблона CPE. Вы можете внести локальные изменения в конфигурацию устройства перед активацией.
   - **Описание**.
   - **Тенант**. Основной тенант. В качестве значения для этого параметра вы также можете указать пул экземпляров SD-WAN или отдельный экземпляр из пула.
   - **Клиентский тенант**. Тенант организации вашего клиента.
   - **Шаблон UNI**. Шаблон UNI, который требуется применить к устройству.

- **Шаблон CPE**. 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*.

Действия, которые вы можете предпринять дальше определяются значением, которое вы выбрали 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. Если вы включаете функции автоматического удаления и деактивации на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

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.

   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.

   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 **Включено** или **Выключено**.

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.

Если требуется, вы можете назначить теги одному или нескольким устройствам CPE одновременно. Обратите внимание, что для назначения тега устройство должно находиться в статусе *Зарегистрировано*.

Kaspersky SD-WAN не поддерживает назначение двух одинаковых тегов одному устройству CPE.

Чтобы назначить тег устройству CPE:

1. Выполните 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 +.

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**.

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.

Инструмент конфигурации VNF, развернутых оркестратором.

Чтобы настроить параметры подключения VNFM к консоли устройства CPE:

1. В области настройки шаблона CPE выберите вкладку **Скрипты**.
2. В открывшемся окне укажите параметры подключения VNFM к устройству CPE:
   - **Имя пользователя по умолчанию**. Имя пользователя для авторизации VNFM в консоли устройства. Максимальная длина: 255 символов.
   - **SSH-порт**. Номер порта для подключения VNFM к консоли устройства CPE.
   - **Пароль по умолчанию**. 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 укажите параметры скрипта:
   - **Имя**. Максимальная длина: 255 символов.
   - **Тайм-аут (сек.)**. Время в секундах, по прошествии которого VNFM перестает предпринимать попытки запуска скрипта, который не запустился с первого раза.
   - **Исполнитель скрипта**.

     Доступные значения:
     - **Ansible**.
     - **Shell**.
     - **Expect**.
     - **Пользовательский**. Использовать собственный интерпретатор в **VNFM**. При выборе этого значения вам нужно ввести путь к интерпретатору в отобразившемся поле **Пользовательский исполнитель**.

Инструмент конфигурации VNF, развернутых оркестратором.

- **Стадия**. Стадия работы устройства CPE, на которой требуется запускать скрипт.

  Доступные значения:

  - **Регистрация**.
  - **Удаление**.
  - **Вручную**. Запускать скрипт только вручную.

- **Авторизация**. Метод авторизации VNFM в консоли устройства CPE.

  Доступные значения:

  - **SSH-ключ**. VNFM использует SSH-ключ.

    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.

- **Повторный запуск**. Флажок, позволяющий запускать скрипт каждый раз при перезагрузке устройства CPE.
- **Скрипт**. Путь к файлу со скриптом или к файлу-сценарию Ansible playbook.
- **Файл**. Путь к дополнительным файлам, необходимым для выполнения скрипта, если требуется. Поддерживаемые форматы архивов с файлами: TAR.GZ и ZIP.

4. Нажмите на кнопку **Сохранить**.

   Скрипт отобразится в таблице со скриптами.

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 сразу несколько скриптов. Например, если вы добавили два скрипта, и каждый из них автоматически запускается при регистрации устройства, порядок запуска определяет, какой скрипт 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 запустите скрипт на всех использующих шаблон устройствах или только на устройствах с определенными тегами:
      - Нажмите на кнопку **Запустить скрипт на всех связанных устройствах CPE**.
      - Нажмите на кнопку **Запустить скрипт на всех связанных устройствах CPE с указанными тегами** и укажите теги.
   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 определенными 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 укажите параметры отложенной задачи:
   - **Тип**. Вам нужно выбрать **Отложенный запуск скрипта**.
   - **Имя**.
   - **Выберите скрипты**. Способ выбора устройств CPE, на которых требуется запустить скрипт.

     Доступные значения:

     - **All CPE with selected template**. Скрипт требуется запустить на всех использующих выбранный шаблон устройствах.
     - **All CPE with selected template and specific tags**. Скрипт требуется запустить на использующих выбранный шаблон устройствах с определенными тегами.
     - **Specific CPE with selected template**. Скрипт требуется запустить на отдельных использующих выбранный шаблон устройствах.
   - **Шаблон CPE** и **Скрипты**. Параметры, позволяющие выбрать скрипт, который требуется запустить.
   - **CPE**. Устройства, на которых требуется запустить скрипт. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Выберите скрипты** вы выбрали **Specific CPE with selected template**.
   - **Теги**. Теги устройств, на которых требуется запустить скрипт. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Выберите скрипты** вы выбрали **All CPE with selected template and specific tags**.
   - **Дата и время выполнения**. Дата и время для выполнения отложенной задачи.
4. Нажмите на кнопку **Добавить**.

Скрипт будет запущен на устройствах CPE в указанное время.

Настройка транспортных путей

Вы можете настраивать параметры используемых транспортных путей в шаблоне CPE или на отдельном устройстве. Обратите внимание, что на отдельном устройстве невозможно изменить значение коэффициента разброса стоимости (англ. cost variance multiplier).

Чтобы указать параметры используемых транспортных путей:

1. В области настройки шаблона CPE или отдельного устройства выберите вкладку **Multipathing**.
2. Укажите параметры транспортных путей:
   - **Максимум транспортных путей**. Максимальное количество транспортных путей, поддерживаемое устройством CPE. Диапазон значений: от 1 до 16.
   - **Максимум Auto-SPF**. Максимальное количество транспортных путей типа Auto-SPF, поддерживаемое устройством CPE. Транспортные пути типа Auto SPF автоматически рассчитываются контроллером SD-WAN. Диапазон значений: от 1 до 16.
   - **Множитель разброса стоимости**. 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.

     Значение этого коэффициента невозможно изменить на отдельных устройствах CPE.

   - **Включить балансировку трафика с учетом веса**. Флажок, определяющий как трафик распределяется по транспортным путям сегмента:
     - Если флажок установлен, трафик распределяется примерно пропорционально значению атрибута веса (Path.weight).
     - Если флажок снят, трафик распределяется равномерно и значение атрибута веса для всех транспортных путей равно 1.
3. Вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона или устройства CPE.

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. Если вы настраиваете подключение к сети SD-WAN на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
3. Укажите параметры подключения:
   - **IP/FQDN оркестратора**. Максимальная длина: 50 символов.
   - **Протокол оркестратора**. Протокол для подключения устройства CPE к оркестратору.

     Доступные значения:
     - **http**;
     - **https**.
   - **Порт оркестратора**. Номер порта оркестратора. Диапазон значений: от 0 до 65535.
   - **OpenFlow-транспорт**. Протокол для установления OpenFlow-соединения между устройством CPE и контроллером SD-WAN.

     Доступные значения:
     - **tcp**;
     - **ssl**.
   - **Перезагрузить, если контроллеры недоступны**. Параметр, определяющий, требуется ли перезагружать устройство CPE при потере связи с контроллером SD-WAN.

     Допустимые значения:
     - **Да**.
     - **Нет**.
   - **Тайм-аут до перезагрузки**. Время в секундах, по прошествии которого устройство CPE будет перезагружено при потере связи с контроллером SD-WAN. Диапазон значений: от 60 до 2 073 600. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Перезагрузить, если контроллеры недоступны** вы выбрали **Да**.
   - **Приоритетный интерфейс управления**. Параметр, определяющий, каким образом выполняется переключение основной сессии для обеспечения взаимодействия устройства CPE с контроллерами SD-WAN.

     Доступные значения:
     - **Random**. Новая сессия выбирается случайно.

- **<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.

- **Обратное переключение**. Флажок, позволяющий выполнять обратное переключение на предыдущую сессию при ее восстановлении по истечении указанного вами времени. Вы можете указать время в секундах в поле **Тайм-аут.** Если флажок снят, обратное переключение на предыдущую основную сессию не происходит.

- **Интервал обновления (сек.)**. 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.

- **URL ZTP**. 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. На данный момент поддерживается 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. Если вы создаете интерфейс SD-WAN на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
3. Нажмите на кнопку **+ Добавить интерфейс**.
4. В открывшемся окне укажите параметры интерфейса SD-WAN:
   - **OpenFlow-интерфейс**. Номер OpenFlow-интерфейса, который требуется создать на виртуальном коммутаторе устройства CPE.
   - **Интерфейс (псевдоним)**. Псевдоним сетевого интерфейса, с которым требуется связать OpenFlow-интерфейс.
   - **Максимальная скорость**. Максимальная скорость интерфейса SD-WAN в МБит в секунду. Диапазон значений: от 1 до 100000.
   - **IP для отслеживания**. IP-адрес хоста, доступность которого определяет доступность интерфейса SD-WAN. Для добавления хоста введите его адрес и нажмите на кнопку **+ Добавить**.
   - **Надежность**. Количество хостов, которые должны оставаться доступными, чтобы интерфейс SD-WAN считался доступным.

     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.

   - **Интервал**. Интервал в секундах для проведения тестов интерфейса SD-WAN. Диапазон значений: от 1 до 600.
   - **Количество**. Количество проверок доступности для каждого из указанных хостов в рамках одного теста интерфейса SD-WAN. Диапазон значений: от 1 до 600.

- **Тайм-аут**. Время в миллисекундах, в течение которого интерфейс SD-WAN ожидает от хостов эхо-ответа после отправления эхо-запроса. Диапазон значений: от 1 до 100000.
- **Down**. Интервал в секундах для проведения тестов интерфейса SD-WAN, если он становится недоступным. Диапазон значений: от 1 до 600.
- **Up**. Интервал в секундах для проведения тестов интерфейса SD-WAN, если он снова становится доступным. Диапазон значений: от 1 до 600.
- **Мониторинг скорости**. Параметр, позволяющий проверять, ограничивается ли скорость интерфейса SD-WAN оператором мобильной связи.

  Доступные значения:

  - **Да**.
  - **Нет**.

5. Если требуется, выберите вкладку **QoS** и настройте очереди трафика для интерфейса SD-WAN:
   - **Изменить ToS**. Параметр, позволяющий изменить значение Type of Service внешних заголовков пакетов трафика каждой очереди. Вы не можете указать значение для этого параметра при настройке очередей трафика для LAN-интерфейса SD-WAN.
   - **Минимум Скорость, %**. Минимальная 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.
   - **Максимум Скорость**, **%**. Максимальная 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.
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. Если вы создаете сетевой интерфейс на отдельном устройстве CPE, выполните следующие действия:

   - Установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

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

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

4. В открывшемся окне укажите параметры сетевого интерфейса:

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

- **Псевдоним**. Параметр, позволяющий сослаться на сетевой интерфейс позже при создании интерфейса SD-WAN. Максимальная длина: 15 символов.

  Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

- **Имя интерфейса**. Физический интерфейс 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.
- **Мост**. Флажок, позволяющий создать мост из интерфейсов, указанных в поле **Имя интерфейса**.
- **Протокол**. Параметр, определяющий, каким образом сетевому интерфейсу назначается IP-адрес. Для создания сетевого интерфейса с автоматическим назначением IP-адреса по протоколу DHCP выберите **DHCP client**.
- **Автоматическое включение**. Флажок, позволяющий автоматически включать сетевой интерфейс одновременно с устройством CPE.
- **Назначать IP, маршрут и шлюз**. Флажок, позволяющий автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.
- **Использовать маршрут по умолчанию**. Флажок, позволяющий использовать на сетевом интерфейсе маршрут по умолчанию, получаемый по протоколу DHCP.
- **DNS-серверы**. Блок для указания IP-адресов DNS-серверов, используемых в вашей сети. Для добавления адреса нажмите на кнопку **+ Добавить** и укажите его в отобразившемся поле.
- **Переопределить MAC**. MAC-адрес сетевого интерфейса. Введенное значение заменяет MAC-адрес по умолчанию.
- **Переопределить MTU**. MTU на сетевом интерфейсе. Введенное значение заменяет MTU по умолчанию.
- **Метрика маршрута**. Если вы создаете первый WAN-интерфейс, вам нужно ввести `100` в этом поле. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

- Сетевой интерфейс со статическим IPv4-адресом.

- **Псевдоним**. Параметр, позволяющий сослаться на сетевой интерфейс позже при создании интерфейса SD-WAN. Максимальная длина: 15 символов.

  Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

- **Имя интерфейса**. Физический интерфейс 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.

- **Мост**. Флажок, позволяющий создать мост из физических интерфейсов, указанных в поле **Имя интерфейса**.

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

- **Автоматическое включение**. Флажок, позволяющий автоматически включать сетевой интерфейс одновременно с устройством CPE.

- **Назначать IP, маршрут и шлюз**. Флажок, позволяющий автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.

- **IPv4-адрес**. Вы можете ввести несколько адресов через пробел.

- **Маска подсети IPv4**. Маска IPv4-адреса.

- **IPv4-шлюз**. IP-адрес шлюза по умолчанию.

- **IPv4-трансляция**. Широковещательный адрес. Если вы не указываете значение для этого параметра, оно генерируется автоматически.

- **DNS-серверы**. Блок для указания IP-адресов DNS-серверов, используемых в вашей сети. Для добавления адреса нажмите на кнопку **+ Добавить** и укажите его в отобразившемся поле.

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

- **Переопределить MTU**. MTU на сетевом интерфейсе. Введенное значение заменяет MTU по умолчанию.

- **Метрика маршрута**. Если вы создаете первый WAN-интерфейс, вам нужно ввести `100` в этом поле. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

- **DHCP-сервер**. Режим работы используемого DHCP-сервера.

  Доступные значения:

  - **Disabled**.

- **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:

- **Первый IP**. IP-адрес, с которого требуется начать выдачу адресов клиентам.
- **Лимит**. Максимальное количество IP-адресов, которое может быть выдано клиентам. Диапазон значений: от 1 до 250.
- **Время аренды**. 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`.
- **DHCP-опции**. Блок для указания DHCP-опций. Для добавления опции нажмите на кнопку **+ Добавить** и введите имя опции в отобразившемся поле. Максимальная длина: 250 символов.

- Сетевой интерфейс со статическим IPv6-адресом.

- **Псевдоним**. Параметр, позволяющий сослаться на сетевой интерфейс позже при создании интерфейса SD-WAN. Максимальная длина: 15 символов.

  Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

- **Имя интерфейса**. Физический интерфейс 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.

- **Мост**. Флажок, позволяющий создать мост из физических интерфейсов, указанных в поле **Имя интерфейса**.

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

- **Автоматическое включение**. Флажок, позволяющий автоматически включать сетевой интерфейс одновременно с устройством CPE.

- **Назначать IP, маршрут и шлюз**. Флажок, позволяющий автоматически назначать сетевому интерфейсу IP-адрес, маршрут и шлюз по умолчанию. Назначение происходит даже в случае отсутствия подключения к сетевому интерфейсу.

- **IPv6-адрес**. Вы можете ввести несколько адресов через пробел.

- **IPv6-суффикс**. Максимальная длина: 30 символов.

- **IPv6-шлюз**. IP-адрес шлюза по умолчанию.

- **Длина префикса**. Длина IPv6-префикса. Диапазон значений: 12 до 127.

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

- **IPv6-префикс**. Максимальная длина: 30 символов.

- **Класс IPv6**. Блок для указания классов IPv6-префиксов, которые будет принимать сетевой интерфейс. Для добавления класса нажмите на кнопку **+ Добавить** и введите имя класса в отобразившемся поле. Максимальная длина: 256 символов.

- **DNS-серверы**. Блок для указания IP-адресов DNS-серверов, используемых в вашей сети. Для добавления адреса нажмите на кнопку **+ Добавить** и укажите его в отобразившемся поле.

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

- **Переопределить MTU**. MTU на сетевом интерфейсе. Введенное значение заменяет MTU по умолчанию.

- **Метрика маршрута**. Если вы создаете первый WAN-интерфейс, вам нужно ввести `100` в этом поле. Для каждого следующего WAN-интерфейса требуется увеличивать значение на 1. Например, для второго WAN-интерфейса введите `101`.

- **DHCP-сервер**. Режим работы используемого DHCP-сервера.

  Доступные значения:

  - **Disabled**.
  - **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:

- **Первый IP**. IP-адрес, с которого требуется начать выдачу адресов клиентам.
- **Лимит**. Максимальное количество IP-адресов, которое может быть выдано клиентам. Диапазон значений: от 1 до 250.
- **Время аренды**. 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`.
- **DHCP-опции**. Блок для указания DHCP-опций. Для добавления опции нажмите на кнопку **+ Добавить** и введите имя опции в отобразившемся поле. Максимальная длина: 250 символов.

- Сетевой интерфейс для подключения к беспроводной сети.

- **Псевдоним**. Параметр, позволяющий сослаться на сетевой интерфейс позже при создании интерфейса SD-WAN. Максимальная длина: 15 символов.

  Вам нужно ввести значение в формате sdwan<номер интерфейса>. Например, при создании сетевого интерфейса, на который будет ссылаться первый интерфейс SD-WAN, введите `sdwan1`.

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

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

- **APN**. Идентификатор APN оператора связи, выпустившего SIM-карту, установленную в модеме. Максимальная длина: 30 символов.

- **Тип аутентификации**.

  Доступные значения:

  - **PAP**. Использовать аутентификацию Password Authentication Protocol.
  - **CHAP**. Использовать аутентификацию Challenge Handshake Authentication Protocol.
  - **BOTH**. Одновременное использовать PAP и CHAP-аутентификацию.
  - **None**. Не использовать аутентификацию.

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

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

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

- **Задержка**. 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.

- **Режимы**. Блок для указания сетевых режимов, которые будут использоваться на сетевом интерфейсе. Для добавления сетевого режима нажмите на кнопку **+ Добавить**.

  Доступные значения:

  - **All**. Использовать все доступные сетевые режимы.
  - **LTE**.
  - **UMTS**.
  - **GSM**.
  - **CDMA**.

- **TD-SCDMA**.

- **Профиль подключения**. Индекс профиля подключения, который сетевой интерфейс должен использовать вместо идентификатора APN. Максимальная длина: 30 символов.

- **IP-стек**.

  Доступные значения:

  - **IP (for IPv4)**. Использовать на сетевом интерфейсе стек протокола IPv4.

  - **IPV6 (for IPv6)**. Использовать на сетевом интерфейсе стек протокола IPv6.

  - I**PV4V6 (for dual-stack)**. Использовать на сетевом интерфейсе двойной стек IPv4 и IPv6.

- **IPv4 через DHCP**. Флажок, позволяющий автоматически 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)**.

- **IPv6 через DHCP**. Флажок, позволяющий автоматически 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)**.

- **Автоподключение**. Флажок, позволяющий автоматически подключать модем к сети.

- **PLMN**. Идентификатор PLMN оператора связи. Первые три цифры идентификатора PLMN являются кодом страны, а вторые три цифры – кодом мобильной сети.

- **Тайм-аут**. Время в секундах, в течение которого сетевой интерфейс должен ожидать выполнения операций на SIM-карте, установленной в модеме. Максимальное значение: 20.

- **Серийный номер**. Последовательный порт (англ. serial port) модема. Максимальная длина: 50 символов.

- **Метрика маршрута**. Если вы создаете первый WAN-интерфейс, вам нужно ввести `100` в этом поле. 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.

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 решения 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 укажите параметры сервисного интерфейса:

   - **Тип**. Тип инкапсуляции на сервисном интерфейсе.

     Доступные значения:

     - **Access**.
     - **VLAN**.
     - **Q-in-Q**.
     - **ACL**. Используется для создания ACL-интерфейса.

   - **VLAN ID**. Внешняя метка VLAN. Диапазон значений: от 1 до 4094. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Тип** вы выбрали **VLAN** или **Q-in-Q**.
   - **Внутренний VLAN ID**. Внутренняя метка VLAN. Диапазон значений: от 1 до 4094. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Тип** вы выбрали **Q-in-Q**.
   - **Описание**.

5. Нажмите на кнопку **Сохранить**.

Сервисный интерфейс отобразится в таблице.

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 решения 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 укажите параметры ACL-интерфейса:

   - **Тип**. Тип инкапсуляции на сервисном интерфейсе. Для создания ACL-интерфейса выберите **ACL**.
   - **Сервисный интерфейс**. Сервисный интерфейс, поверх которого требуется создать ACL-интерфейс.
   - **Фильтр трафика**. Фильтр трафика для ACL-интерфейса. Вы можете использовать один фильтр трафика для нескольких ACL-интерфейсов.

- **Порядковый номер**. Трафик, поступающий в сервисный интерфейс, в первую очередь 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.

- **Описание**.

5. Нажмите на кнопку **Сохранить**.

ACL-интерфейс отобразится в таблице.

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.
4. Нажмите на созданный шаблон UNI и выберите вкладку **UNI**.
5. Нажмите на кнопку **+ Добавить шаблон UNI**.
6. В открывшемся окне укажите параметры UNI:

   - **Имя**.
   - **OpenFlow-интерфейс**. Номер OpenFlow-интерфейса, поверх которого требуется создать UNI.
   - **Тип сегментации**. Тип инкапсуляции на UNI.

     Доступные значения:

     - **Access**.
     - **VLAN**.
     - **Q-in-Q**.
   - **VLAN ID**. Внешняя метка VLAN. Диапазон значений: от 1 до 4094. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Тип сегментации** вы выбрали **VLAN** или **Q-in-Q**.
   - **Внутренний VLAN ID**. Внутренняя метка VLAN. Диапазон значений: от 1 до 4094. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Тип сегментации** вы выбрали **Q-in-Q**.

7. Нажмите на кнопку **Добавить**.

   UNI отобразится в таблице.

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 укажите параметры UNI:
   - **Имя**.
   - **Порт**. OpenFlow-интерфейс, поверх которого требуется создать UNI.
   - **Тип сегментации**. Тип инкапсуляции на UNI.

     Доступные значения:

     - **Access**.
     - **VLAN**.
     - **Q-in-Q**.
   - **VLAN ID**. Внешняя метка VLAN. Диапазон значений: от 1 до 4094. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Тип сегментации** вы выбрали **VLAN** или **Q-in-Q**.
   - **Внутренний VLAN ID**. Внутренняя метка VLAN. Диапазон значений: от 1 до 4094. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Тип сегментации** вы выбрали **Q-in-Q**.
   - **QoS**. Правило качества обслуживания для UNI.
4. Нажмите на кнопку **Добавить**.

   UNI отобразится в таблице.

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 решения перейдите в раздел **Группы OF-интерфейсов**.
2. Нажмите на кнопку **+ Добавить группу OF-интерфейсов**.
3. В открывшемся окне укажите параметры группы OpenFlow-интерфейсов:
   - **Имя**.
   - **Коммутатор** и **Порт**. Параметры, позволяющие выбрать OpenFlow-интерфейс, который вы хотите добавить в группу.
4. Нажмите на кнопку **Создать**.

Группа OpenFlow-интерфейсов отобразится в таблице.

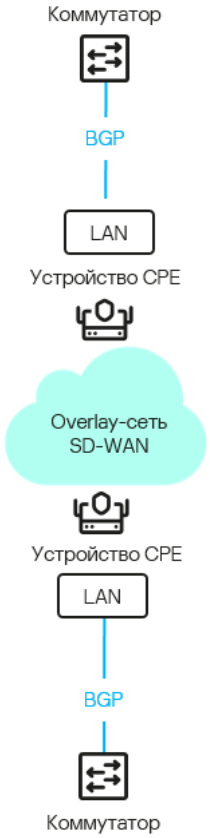
Протокол динамической маршрутизации BGP

Kaspersky SD-WAN поддерживает использование протокола динамической маршрутизации BGP (Border Gateway Protocol) для обмена маршрутной информацией между подключенными к вашей сети SD-WAN устройствами CPE, а также со сторонними сетевыми устройствами. Вы можете устанавливать как внутренние сессии iBGP (internal BGP), так и внешние сессии eBGP (external BGP).

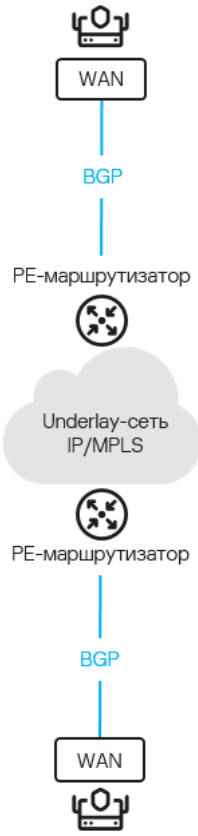
Также поддерживается установка динамических TCP-сессий с группами BGP-соседей (англ. BGP peer groups). Установив динамическую TCP-сессию, вам не нужно создавать отдельных BGP-соседей (англ. BGP peers).

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

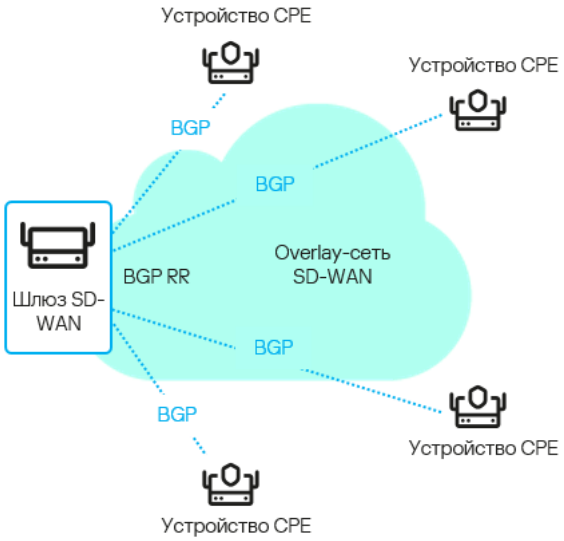
- Подключение нескольких клиентских площадок к сети L3 SD-WAN по BGP.



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



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



Настройка протокола BGP

Вы можете 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. Если вы настраиваете BGP на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
3. В раскрывающемся списке **BGP** выберите **Включено** или **Выключено**.
4. Укажите параметры BGP:
   - **AS**. Номер вашей автономной системы. Диапазон значений: от 1 до 4 294 967 295.
   - **ID устройства CPE**.
   - **Лимит маршрутов**. Максимальное количество записей в таблице маршрутизации устройства CPE. Диапазон значений: от 1 до 8.
   - **Всегда сравнивать MED**. Флажок, позволяющий устройству CPE сравнивать атрибут MED (multi-exit discriminator) маршрутов, анонсированных из разных автономных систем.

     Вам нужно убедиться, что этот параметр настроен одинаково на всех устройствах CPE в вашей автономной системе. В противном случае при обмене маршрутной информацией могут возникать петли маршрутизации.

   - **Graceful Restart**. Флажок, позволяющий устройству CPE оставаться в таблицах маршрутизации BGP-соседей при перезагрузке. Таким образом, после перезагрузки устройство может продолжать участвовать в обмене маршрутной информацией.
   - **IPv4 unicast-маршруты по умолчанию**. Флажок, позволяющий устройству CPE по умолчанию обмениваться IPv4-маршрутами с BGP-соседями.

- **BGP-таймеры**. Флажок, позволяющий настроить BGP-таймеры.

  Если вы установили этот флажок, укажите следующие параметры:

  - **Keepalive**. Интервал времени в секундах для отправки устройством CPE keepalive-сообщений BGP-соседям. Диапазон значений: от 0 до 65535.
  - **Holdtime**. 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.

- **Перераспределение маршрутов**. Типы маршрутов, которые устройство CPE может анонсировать BGP-соседям. Для выбора типа маршрута установите рядом с ним флажок.

  Вы можете указать следующие параметры для каждого типа маршрутов:

  - **Карта маршрутизации**. Карта маршрутизации для анонсируемых маршрутов.
  - **Метрика**. Метрика для анонсируемых маршрутов. Диапазон значений: от 0 до 4 294 967 295.

- **Сети**. Сети, которые устройство CPE должно анонсировать BGP-соседям. Для добавления сети нажмите на кнопку **+ Сеть** и укажите следующие параметры:

  - **Сеть**. IP-адрес и маска подсети.
  - **Карта маршрутизации**. Карта маршрутизации для маршрутов.

5. Если требуется, выполните следующие действия:

   - Создайте списки управления доступом.
   - Создайте списки префиксов.
   - Создайте карты маршрутизации.

6. Создайте BGP-соседей 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, к которым принадлежат маршруты.

Правила в списке управления доступом могут разрешать или запрещать анонсирование маршрутов, принадлежащих к определенной сети. Каждое правило имеет порядковый номер. Устройство CPE будет сравнивать информацию о сети, к 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. Если вы создаете список управления доступом на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

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**, чтобы добавить правило в список управления доступом.

6. Укажите параметры правила:

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

   - **Сеть**. Тип правила.

     Доступные значения:

     - **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.

   - **Действие**. Действие, которое правило должно применять к маршрутам.

     Доступные значения:

     - **Permit**. Разрешать анонсирование маршрутов.

     - **Deny**. Запрещать анонсирование маршрутов.

7. Нажмите на кнопку **Сохранить**.

   Список управления доступом отобразится в таблице.

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. Если вы создаете список префиксов на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
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**, чтобы добавить правило в список префиксов.
6. Укажите параметры правила:
   - **Порядковый номер**. Правило с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 4 294 967 295.
   - **Сеть**. Тип правила.

     Доступные значения:
     - **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.
   - **Действие**. Действие, которое правило должно применять к маршрутам.

     Доступные значения:
     - **Permit**. Разрешать анонсирование маршрутов.
     - **Deny**. Запрещать анонсирование маршрутов.
   - **Greater or Equal** и **Less or Equal**. Параметры, позволяющие задать диапазон префиксов. Диапазон значений для каждого из параметров: от 0 до 32.
7. Нажмите на кнопку **Сохранить**.

   Список префиксов отобразится в таблице.
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. Если вы создаете карту маршрутизации на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

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**, чтобы добавить правило в карту маршрутизации.

6. Укажите параметры правила:

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

   - **Действие**. Действие, которое правило должно применять к маршрутам.

     Доступные значения:

     - **Permit**. Разрешать анонсирование маршрутов.

     - **Deny**. Запрещать анонсирование маршрутов.

   - **Условие**. Условие, выполнение которого необходимо для применения правила к маршруту.

     Доступные значения:

     - **None**. Применять правило ко всем маршрутам. Вы не можете изменять значения атрибутов с помощью этого правила.

     - **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**.

   - **Изменять атрибут**. Атрибут, значение которого требуется изменять при применении правила к маршруту.

     Доступные значения:

     - **None**. Не изменять значения атрибутов.

     - **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.

- **Новое значение**. 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.

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. Если вы создаете BGP-соседа на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
3. Нажмите на кнопку **+ Добавить BGP-соседа**.
4. В открывшемся окне укажите параметры BGP-соседа:
   - **Имя**. Максимальная длина: 50 символов.
   - **Выключить BGP-соседа**. Флажок, позволяющий не устанавливать TCP-сессию при создании BGP-соседа.
   - **Адрес соседа**. IP-адрес BGP-соседа.
   - **AS**. Номер автономной системы BGP-соседа. Диапазон значений: от 1 до 4 294 967 295.
   - **Описание**.
   - **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.
   - **Loopback-интерфейс**. IP-адрес loopback-интерфейса, который устройство CPE должно передавать BGP-соседу при установлении TCP-сессии.

- **Хопы для eBGP**. Количество хопов (англ. hops) между устройством CPE и BGP-соседом. Параметр используется, если TCP-сессия устанавливается не напрямую. Диапазон значений: от 1 до 255.

- **Уникальные BGP-таймеры**. Флажок, позволяющий настроить BGP-таймеры.

  Если вы установили флажок, укажите следующие параметры:

  - **Keepalive**. Интервал времени в секундах для отправки устройством CPE keepalive-сообщений BGP-соседу. Диапазон значений: от 0 до 65535.

  - **Holdtime**. Время в секундах, в течение которого устройство CPE должно ожидать получения keepalive-сообщений от BGP-соседа. Если в течение указанного времени от BGP-соседа не поступает keepalive-сообщений, устройство считает его недоступным. Диапазон значений: от 0 до 65535.

- **Включить BFD**. Флажок, позволяющий использовать протокол BFD для обнаружения сбоев в TCP-сессии.

  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 укажите требуемые параметры:

   - **Soft-reconfiguration inbound**. Флажок, позволяющий хранить анонсированные BGP-соседом маршруты локально на устройстве CPE.

     Использование этой функции снижает количество доступной на устройстве памяти.

   - **Неизменный атрибут AS path**. Флажок, позволяющий не изменять атрибут AS path маршрутов, которые устройство CPE анонсирует BGP-соседу.

   - **Разрешить AS in**. Флажок, позволяющий устройству CPE получать от BGP-соседа маршруты с атрибутом AS path, значением которого является номер автономной системы этого устройства.

   - **Неизменный атрибут Next Hop**. Флажок, позволяющий не изменять атрибут next hop маршрутов, которые устройство CPE анонсирует BGP-соседу.

   - **Собственный IP как Next Hop**. Флажок, позволяющий использовать IP-адрес устройства CPE в качестве атрибута next-hop при анонсировании маршрутов BGP-соседу.

   - **Неизменный атрибут MED**. Флажок, позволяющий не изменять атрибут MED маршрутов, которые устройство CPE анонсирует BGP-соседу.

   - **Клиент Route Reflector**. Флажок, позволяющий 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.

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

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

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

- **Отправлять community**. Флажок, позволяющий устройству CPE анонсировать BGP-соседу маршруты с атрибутом community.

  Если вы установили этот флажок, выберите одно из следующих значений в раскрывающемся списке:

  - **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.

- **Отправлять маршрут по умолчанию**. Флажок, позволяющий устройству CPE отправлять BGP-соседу маршрут по умолчанию. Маршрутом по умолчанию является IP-адрес 0.0.0.0.

  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 укажите требуемые параметры:

   - **Карта маршрутизации**. Блок для указания карт маршрутизации для фильтрации маршрутной информации.

     Вы можете указать следующие параметры:

     - **Входящие**. Карта маршрутизации, которую BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.
     - **Исходящие**. Карта маршрутизации, которую устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

   - **Список префиксов**. Блок для указания списков префиксов для фильтрации маршрутной информации.

     Вы можете указать следующие параметры:

     - **Входящие**. Список префиксов, который BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.
     - **Исходящие**. Список префиксов, который устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

   - **Список управления доступом**. Блок для указания списков управления доступом для фильтрации маршрутной информации.

     Вы можете указать следующие параметры:

     - **Входящие**. Список управления доступом, который BGP-сосед должен использовать при анонсировании маршрутов устройству CPE.
     - **Исходящие**. Список управления доступом, который устройство CPE должно использовать при анонсировании маршрутов BGP-соседу.

7. Нажмите на кнопку **Сохранить**.

   BGP-сосед отобразится в таблице.

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. Если вы создаете группу BGP-соседей на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

3. Нажмите на кнопку **+ Добавить группу BGP-соседей**.

4. В открывшемся окне укажите параметры группы BGP-соседей:

   - **Имя**. Максимальная длина: 50 символов.
   - **Выключить группу BGP-соседей**. Флажок, позволяющий не устанавливать TCP-сессию при создании группы BGP-соседей.
   - **BGP Listen Range**. Диапазон IP-адресов группы BGP-соседей, который определяется с помощью префикса.
   - **AS**. Номер автономной системы группы BGP-соседей. Диапазон значений: от 1 до 4 294 967 295.
   - **Описание**.
   - **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.
   - **Loopback-интерфейс**. IP-адрес loopback-интерфейса, который устройство CPE должно передавать группе BGP-соседей при установлении TCP-сессии.
   - **Хопы для eBGP**. Количество хопов (англ. hops) между устройством CPE и группой BGP-соседей. Параметр используется, если TCP-сессия устанавливается не напрямую. Диапазон значений: от 1 до 255.
   - **Уникальные BGP-таймеры**. Флажок, позволяющий настроить BGP-таймеры.

     Если вы установили флажок, укажите следующие параметры:

     - **Keepalive**. Интервал времени в секундах для отправки устройством CPE keepalive-сообщений группе BGP-соседей. Диапазон значений: от 0 до 65535.
     - **Holdtime**. 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.

- **Включить BFD**. Флажок, позволяющий использовать протокол BFD для обнаружения сбоев в TCP-сессии.

  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 укажите требуемые параметры:

   - **Soft-reconfiguration inbound**. Флажок, позволяющий хранить анонсированные группой BGP-соседей маршруты локально на устройстве CPE.

     Использование этой функции снижает количество доступной на устройстве памяти.

   - **Неизменный атрибут AS path**. Флажок, позволяющий не изменять атрибут AS path маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

   - **Разрешить AS in**. Флажок, позволяющий устройству CPE получать от группы BGP-соседей маршруты с атрибутом AS path, значением которого является номер автономной системы этого устройства.

   - **Неизменный атрибут Next Hop**. Флажок, позволяющий не изменять атрибут next hop маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

   - **Собственный IP как Next Hop**. Флажок, позволяющий использовать IP-адрес устройства CPE в качестве атрибута next-hop при анонсировании маршрутов группе BGP-соседей.

   - **Неизменный атрибут MED**. Флажок, позволяющий не изменять атрибут MED маршрутов, которые устройство CPE анонсирует группе BGP-соседей.

   - **Клиент Route Reflector**. Флажок, позволяющий 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.

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

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

   - **Лимит префиксов**. Максимальное количество префиксов, которое группа BGP-соседей может анонсировать устройству CPE. Диапазон значений: от 1 до 4 294 967 295.

   - **Отправлять community**. Флажок, позволяющий устройству CPE анонсировать группе BGP-соседей маршруты с атрибутом community.

     Если вы установили этот флажок, выберите одно из следующих значений в раскрывающемся списке:

     - **All**. Устройство может отправлять группе BGP-соседей все доступные типы атрибута community.

     - **Both**. Устройство может отправлять группе BGP-соседей атрибуты standard community и extended community.

- **Extended**. Устройство может отправлять группе BGP-соседей атрибут extended community.
- **Large**. Устройство может отправлять группе BGP-соседей атрибут large community.
- **Standard**. Устройство может отправлять группе BGP-соседей атрибут standard community.

- **Отправлять маршрут по умолчанию**. Флажок, позволяющий устройству CPE отправлять группе BGP-соседей маршрут по умолчанию. Маршрутом по умолчанию является IP-адрес 0.0.0.0.

  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 укажите требуемые параметры:

   - **Карта маршрутизации**. Блок для указания карт маршрутизации для фильтрации маршрутной информации.

     Вы можете указать следующие параметры:

     - **Входящие**. Карта маршрутизации, которую группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.
     - **Исходящие**. Карта маршрутизации, которую устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.

   - **Список префиксов**. Блок для указания списков префиксов для фильтрации маршрутной информации.

     Вы можете указать следующие параметры:

     - **Входящие**. Список префиксов, который группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.
     - **Исходящие**. Список префиксов, который устройство CPE должно использовать при анонсировании маршрутов группе BGP-соседей.

   - **Список управления доступом**. Блок для указания списков управления доступом для фильтрации маршрутной информации.

     Вы можете указать следующие параметры:

     - **Входящие**. Список управления доступом, который группа BGP-соседей должна использовать при анонсировании маршрутов устройству CPE.
     - **Исходящие**. 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.

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. Если вы настраиваете BFD на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
3. В раскрывающемся списке **BFD** выберите **Включено** или **Выключено**.

   Если вы включили BFD, вам нужно создать BFD-соседа.
4. Нажмите на кнопку **+ Добавить BFD-соседа**.
5. В открывшемся окне укажите параметры BFD-соседа:

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

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. Если вы создаете статический IPv4-маршрут на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

3. Нажмите на кнопку создания статического IPv4-маршрута + и укажите его параметры:

   - **Интерфейс**. Сетевой интерфейс для отправки пакетов трафика на узел назначения.
   - **Маска подсети IPv4**. Маска подсети узла назначения.
   - **Шлюз**. IP-адрес шлюза для маршрутизации трафика.
   - **Метрика**.
   - **MTU**.
   - **Тип**.

     Доступные значения:

     - **unicast**. Стандартный маршрут до узла назначения.
     - **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.

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. Если вы настраиваете протокол VRRP на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

3. В раскрывающемся списке **VRRP** выберите **Включено** или **Выключено**.

   Для создания экземпляра требуется включить VRRP.

4. Нажмите на кнопку **+ Добавить экземпляр VRRP**.

5. В открывшемся окне укажите параметры экземпляра VRRP:

   - **Имя**. Максимальная длина: 16 символов.

   - **VRID**. 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.

- **Интерфейс**. Сетевой интерфейс, которому будет назначен виртуальный IP-адрес.
- **VIP**. Виртуальный IP-адрес для сетевого интерфейса. Вам нужно назначить одинаковый виртуальный IP-адрес сетевым интерфейсам всех устройств CPE, которые требуется объединить в виртуальный маршрутизатор.
- **Состояние**. Роль устройства CPE.

  Доступные значения:

  - **BACKUP**. Резервный VRRP-маршрутизатор.
  - **MASTER**. Основной VRRP-маршрутизатор.
- **Приоритет**. Чем выше значение, введенное в этом поле, тем выше приоритет VRRP-маршрутизатора. 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.
- **Интервал оповещения**. Интервал времени в секундах для отправки VRRP-объявлений. Диапазон значений: от 1 до 60.
- **Оставлять резервным при восстановлении**. Флажок, позволяющий не изменять роль резервного VRRP-маршрутизатора, ставшего основным, даже если прежний основной VRRP-маршрутизатор восстанавливает работу.
- **Unicast-рассылка**. Флажок, позволяющий настроить отправку VRRP-объявлений в виде unicast-сообщений.

  Если вы установили флажок, укажите следующие параметры:

  - **IP основного VRRP-маршрутизатора**.
  - **IP резервного VRRP-маршрутизатора**.
- **Аутентификация**. Флажок, позволяющий указать пароль для аутентификации VRRP-объявлений. Если вы установили этот 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.

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. Если вы создаете группу экземпляров VRRP на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

3. Нажмите на кнопку **+ Добавить группу экземпляров VRRP**.

4. В открывшемся окне укажите параметры группы экземпляров VRRP:

   - **Имя**. Максимальная длина: 16 символов.
   - **Экземпляры VRRP**. Экземпляры, которые требуется добавить в группу.

5. Нажмите на кнопку **Сохранить**.

   Группа экземпляров VRRP отобразится в таблице.

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. Укажите параметры подключения:

   - **Веб-консоль**. Параметр, позволяющий разрешить или запретить пользователям подключаться к веб-консоли устройства CPE.

     Доступные значения:

     - **Enable**. Пользователи могут подключаться к веб-консоли.
     - **Disable**. Пользователи не могут подключаться к веб-консоли.

   - **Порт**. Номер порта для подключения к веб-консоли.
   - **Протокол**. Протокол для подключения к веб-консоли.

     Допустимые значения:

     - **http**;
     - **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. Если вы настраиваете подключение к Syslog-серверу на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
3. Укажите параметры подключения:
   - **Размер файлов журнала, КБ**. Размер файлов журнала на устройстве CPE в КБ. Диапазон значений: от 64 до 2048.
   - **IP или FQDN Syslog-сервера**.
   - **Порт Syslog-сервера**. Диапазон значений: от 0 до 65353.
   - **Протокол Syslog-сервера**. Протокол для передачи файлов журнала на Syslog-сервер.

     Доступные значения:
     - **UDP**.
     - **TCP**.
   - **Префикс для журналов**. 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. Если вы настраиваете подключение к NTP-серверу на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
3. Укажите параметры подключения:
   - **Подключиться к NTP-серверу**. Флажок, позволяющий разрешить или запретить устройству CPE подключаться к NTP-серверу.
   - **NTP-серверы**. Блок для указания IP-адресов или FQDN NTP-серверов. Для добавления адреса нажмите на кнопку **+ Добавить** и введите его в отобразившемся поле. Пример значения: `server 0.pool.ntp.org`.

- **Использовать как NTP-сервер**. Флажок, позволяющий использовать устройство CPE в качестве NTP-сервера.

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 укажите параметры VIM:
   - **Порт**. Номер порта для подключения оркестратора к VIM.
   - **Протокол**. Протокол для подключения оркестратора к VIM.

     Доступные значения:
     - **http**;
     - **https**.
   - **Имя пользователя** Имя пользователя учетной записи OpenStack с правами администратора для авторизации в VIM.
   - **Пароль**. Пароль учетной записи OpenStack с правами администратора для авторизации в VIM.
   - **Проект администратора**. Имя проекта администратора OpenStack для авторизации в VIM.
   - **Домен**. Имя OpenStack-домена.
   - **Физическая VLAN-сеть**. Имя physnet для VLAN-сетей.
   - **За NAT**. Параметр, позволяющий определить, находится ли VIM за NAT.

     Доступные значения:
     - **Включено**. VIM находится за NAT.
     - **Выключено**. VIM не находится за NAT.
   - **Переподписка ЦП**. Коэффициент переподписки при предоставлении виртуальных процессорных ядер.
   - **Переподписка диска**. Коэффициент переподписки дискового пространства.
   - **Переподписка ОЗУ**. Коэффициент переподписки оперативной памяти.

- **Диапазон VLAN ID**. Максимальное количество VLAN для OpenStack. Диапазон значений: от 0 до 4094.

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 установить прошивку на устройстве CPE в следующих разделах/подразделах веб-интерфейса оркестратора:

- **Устройства CPE**. В этом случае вам нужно установить флажки рядом с одним или несколькими устройствами, после чего создать отложенную задачу по обновлению с помощью раскрывающегося списка **Действия**.

- **Планировщик задач**. В этом случае 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.

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 следующих разделах/подразделах веб-интерфейса оркестратора:

- **Устройства CPE**.
- **Планировщик**.

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 одним из следующих способов:
   - В навигационной панели перейдите в раздел **SD-WAN**, установите флажки рядом с устройствами CPE, на которых требуется обновить прошивку, и вверху справа в раскрывающемся списке **Действия** выберите **Обновить прошивку**.
   - В навигационной панели перейдите в раздел **Планировщик** и нажмите на кнопку **+ Отложенная задача**.
2. В открывшемся окне укажите параметры прошивки:
   - **Тип**. Параметр, позволяющий выбрать тип отложенной задачи. Вы можете указать значение для этого параметра только если вы обновляете прошивку в разделе **Планировщик**. Вам нужно выбрать **Обновление прошивки CPE**.
   - **Имя**.
   - **Версия**. Прошивка, которую требуется установить на устройстве CPE.

- **Дата и время выполнения**. Дата и время обновления прошивки.

- **Сохранить конфигурацию CPE**. Флажок, позволяющий сохранить конфигурацию устройства CPE после обновления прошивки.

  Если вы флажок не установлен, после установки прошивки параметры устройства сбрасываются до заводских значений.

- **Принудительное обновление**. Флажок, позволяющий установить прошивку принудительно, даже если внутренняя проверка на устройстве CPE выявляет несовместимость его текущей прошивки с новой.

- **Теги**. Теги устройств CPE, на которых требуется обновить прошивку. Вы можете указать значение для этого параметра только если вы обновляете прошивку в разделе **Планировщик**.

3. Нажмите на кнопку **Далее**, чтобы перейти к следующей группе параметров.

   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 подразделе **Устройства CPE**, нажмите на кнопку **Запланировать**.

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

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

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. Укажите параметры подключения к серверу Zabbix:
   - **URL**. 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`.
   - **Имя пользователя**. 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.
   - **Пароль**. Пароль пользователя для подключения к Zabbix API.
   - **VNF/PNF группа**. Имя группы узлов сети, которую вы создали на сервере Zabbix для мониторинга VNF или PNF. Если вы не создали группу, оркестратор создает ее автоматически.
   - **Группа для устройств CPE**. Имя группы узлов сети, которую вы создали на сервере Zabbix для мониторинга устройств CPE. Если вы не создали группу, оркестратор создает ее автоматически.
   - **Интервал для уведомлений**. Интервал времени в секундах для отправки уведомлений о возникших ошибках с сервера Zabbix. Диапазон значений: от 5 до 600.
3. Снизу от поля **Токен** нажмите на кнопку **Сгенерировать**, чтобы сгенерировать токен, который сервер Zabbix использует для установления безопасного соединения с оркестратором. Безопасность также обеспечивается TLS-сертификатами.

   Вы можете ввести токен вручную, а также просмотреть его, нажав на кнопку просмотра 👁.
4. Если требуется, 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** укажите параметры Zabbix-прокси:

   - **Имя**. Имя сервера Zabbix-прокси. Введенное имя должно совпадать с именем, указанным в параметрах сервера Zabbix-прокси.

   - **IP**. 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. Укажите параметры мониторинга устройства CPE:

   - **Тип мониторинга**.

     Доступные значения:

     - **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. **Шаблон Zabbix**. 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.

- **Экземпляры SD-WAN**. Для просмотра результатов мониторинга всего экземпляра SD-WAN.

Если вы планируете просматривать результаты мониторинга отдельного устройства, перед выполнением этой инструкции требуется настроить параметры мониторинга в примененном к нему шаблоне CPE.

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 следующих разделах/подразделах веб-интерфейса оркестратора:

- **Устройства CPE**.
- **Топология**.
- **Туннели**.

Чтобы включить мониторинг на туннеле:

1. Откройте окно мониторинга туннеля одним из следующих способов:

   - 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**.

   - В дополнительном меню настройки решения 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 решения перейдите в раздел **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 укажите параметры мониторинга:

   - **Установки по умолчанию**. Кнопка, позволяющая использовать пороговые значения мониторинга по умолчанию

   - **Нежелательный**. Флажок, позволяющий отметить туннель как нежелательный. *Нежелательные туннели* не используются при маршрутизации или используются в последнюю очередь, независимо от качества связи.

   - **Интервал обработки ошибок туннеля и статистики использования, сек**. Интервал времени в секундах для измерения количества ошибок на туннеле и уровня его загруженности. Диапазон значений: от 1 до 300.

   - **Включить мониторинг ошибок туннеля**. Флажок, позволяющий указать пороговое значение количества ошибок на туннеле в поле **Уровень критических ошибок туннеля, ошибок/сек**. Диапазон значений: от 1 до 1 000 000.

- **Включить мониторинг использования туннеля**. Флажок, позволяющий указать пороговое значение загруженности туннеля в процентах от установленной скорости сервисного интерфейса в поле **Критический уровень использования туннеля, %**.

- **Качество связи (задержка, джиттер, потеря пакетов), интервал обработки статистики**. Интервал времени в секундах для измерения показателей задержки, джиттера и потери пакетов на туннеле. Диапазон значений:от 1 до 600.

- **Включить мониторинг задержек туннеля**. Флажок, позволяющий указать максимальное время задержки в миллисекундах при передаче пакетов по туннелю в поле **Критический уровень задержек туннеля, мс**. Диапазон значений: от 5 до 1000.

- **Включить мониторинг джиттера туннеля**. Флажок, позволяющий указать максимальное время джиттера в миллисекундах при передаче пакетов по туннелю в поле **Критический уровень джиттера туннеля, мс**. Диапазон значений: от 5 до 1000.

- **Включить мониторинг потерь пакетов туннеля**. Флажок, позволяющий указать максимальный процент потери пакетов на туннеле в поле **Критический уровень потерь пакетов туннеля, %**. Диапазон значений: от 1 до 100.

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 разделе **Устройства CPE**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства.

Построение топологии

Соединение между **устройствами CPE** устанавливается через туннели, которые строятся поверх каналов передачи данных. Туннели являются однонаправленными, поэтому при установлении соединения между двумя устройствами или между устройством и **плоскостью управления сетью** требуется построить как входящий, так и исходящий туннель.

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

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, который вы создаете вручную. Для создания транспортного пути этого типа вам нужно указать параметры туннелей, через которые транспортный путь будет проходить от устройства CPE в начале сегмента до устройства в конце сегмента.

- **Auto-TE**. Автоматически рассчитываемый контроллером SD-WAN транспортный путь, учитывающий указанные вами ограничения (англ. constraints). Ограничениями могут быть значения показателей мониторинга на туннелях, например показатель уровня загрузки туннеля.

Кроме того, транспортные пути могут иметь следующие параметры:

- **Стоимость (англ. Path.cost)**. По умолчанию является суммой стоимости всех туннелей, которые входят в транспортный путь. Вы можете вручную указать стоимость транспортных путей Manual-TE и Auto-TE.

- **Вес (англ. Path.weight)**.

- **Административное состояние (англ. Path.admin.state)**. Вам нужно указать значение параметра вручную. Если этот параметр имеет значение down, транспортный путь не используется.

- **Фактическое состояние (англ. Path.oper.state)**. Зависит от наличия или отсутствия возможности передачи трафика. Если этот параметр имеет значение down, транспортный путь не используется.

Один сегмент может содержать от 2 до 16 транспортных путей и при передаче трафика по умолчанию выбирается наилучший транспортный путь с наименьшим значением атрибута стоимости. Если наилучший транспортный путь недоступен для передачи трафика по техническим причинам, выбирается другой транспортный путь с приближенным значением атрибута 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.

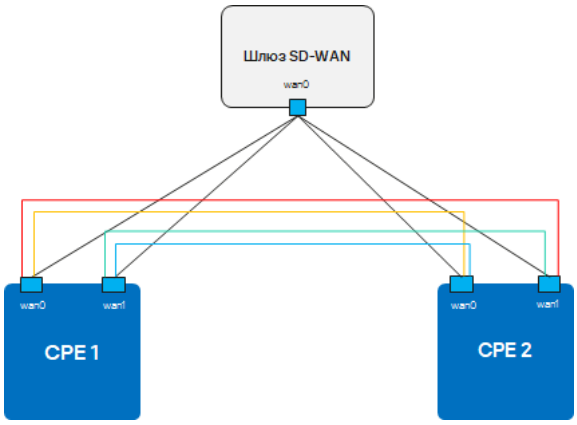
Топологии Full-Mesh и Partial-Mesh

В Kaspersky SD-WAN, помимо топологии Hub-and-Spoke, поддерживаются топологии Full-Mesh и Partial-Mesh. Для реализации этих топологий требуется настройка разрешения администратором сети на динамическое построение прямых туннелей между устройствами CPE.

Как правило, построение прямых туннелей между устройствами CPE позволяет увеличить качественные и количественные характеристики производительности Kaspersky SD-WAN по следующим причинам:

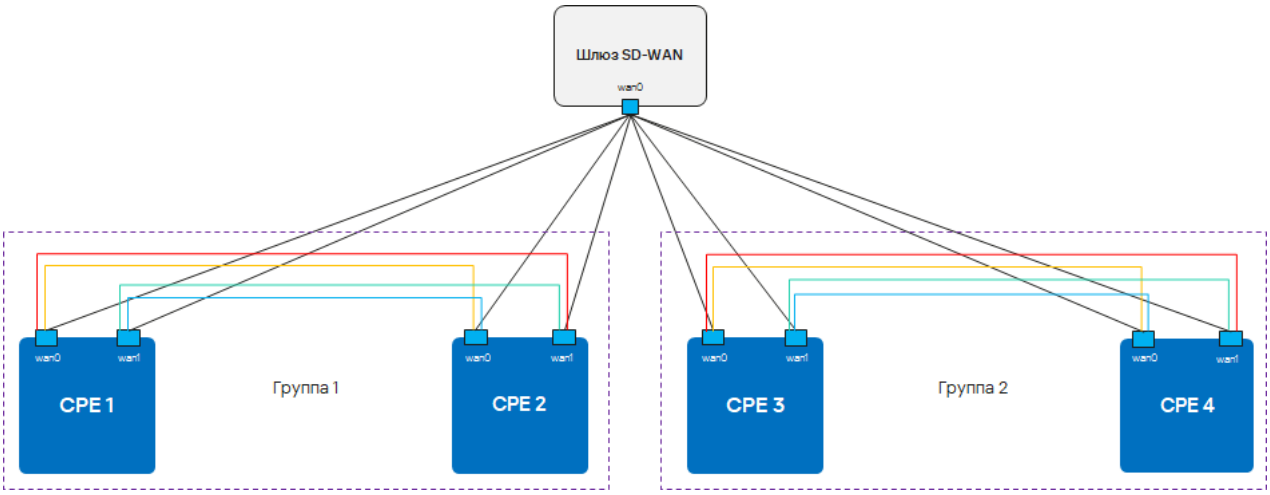
- Качественные характеристики физического канала передачи данных между устройствами CPE, такие как задержка (англ. delay), потеря пакетов (англ. loss) и джиттер (англ. jitter), могут быть лучше, чем в транзитном сценарии CPE1 → шлюз → CPE2 топологии Hub-and-Spoke.
- Пропускная способность прямого физического канала передачи данных между устройствами CPE может быть больше, чем в транзитном сценарии CPE1 → шлюз → CPE2.
- При использовании прямых связей не расходуются ресурсы шлюза, то есть пропускная способность физического канала передачи данных и аппаратные ресурсы самого шлюза.

Пример топологии Full-Mesh приведен на рисунке ниже. В этой топологии все устройства CPE пытаются построить прямые туннели между собой, используя все имеющиеся физические каналы передачи данных. Таким образом, трафик между устройствами CPE1 и CPE2 может пересылаться напрямую. Однако при большом количестве устройств CPE и туннелей такая топология может оказаться чрезвычайно требовательной к ресурсам контроллера SD-WAN.



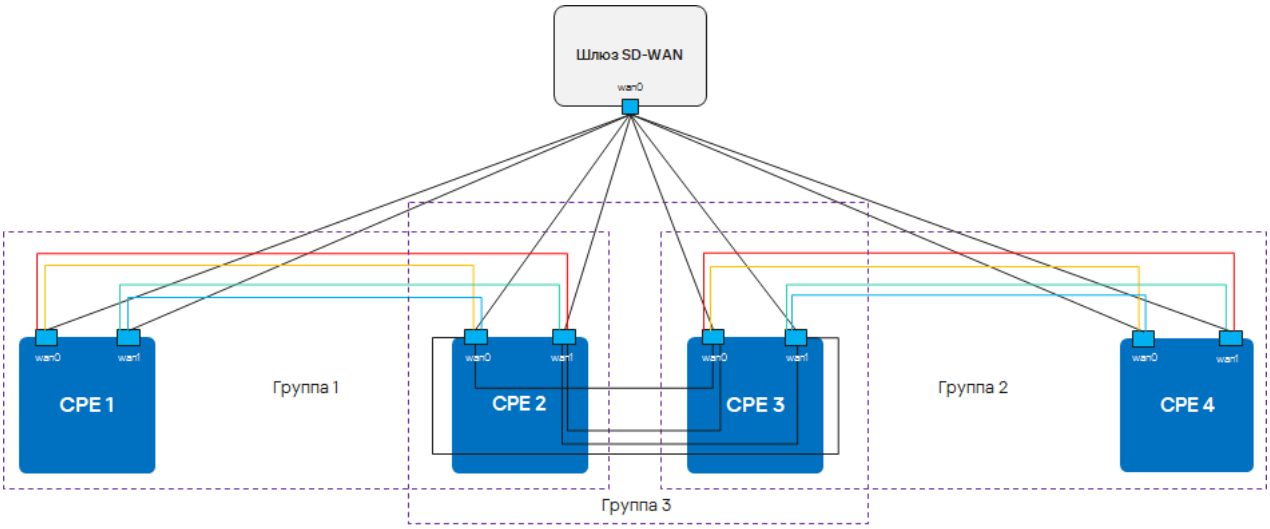
Топология Full Mesh

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.

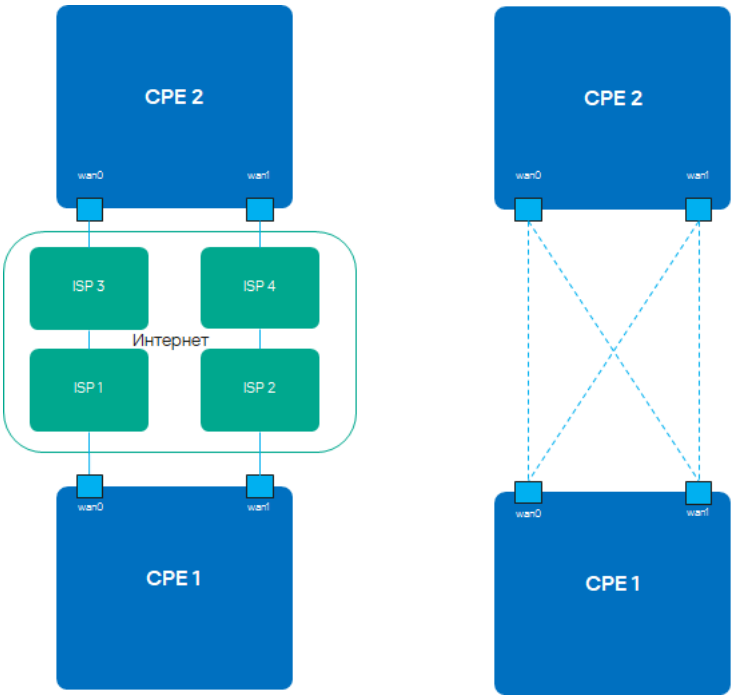


Топология Partial Mesh, устройства CPE входят в несколько групп

Особенности построения туннелей P2P

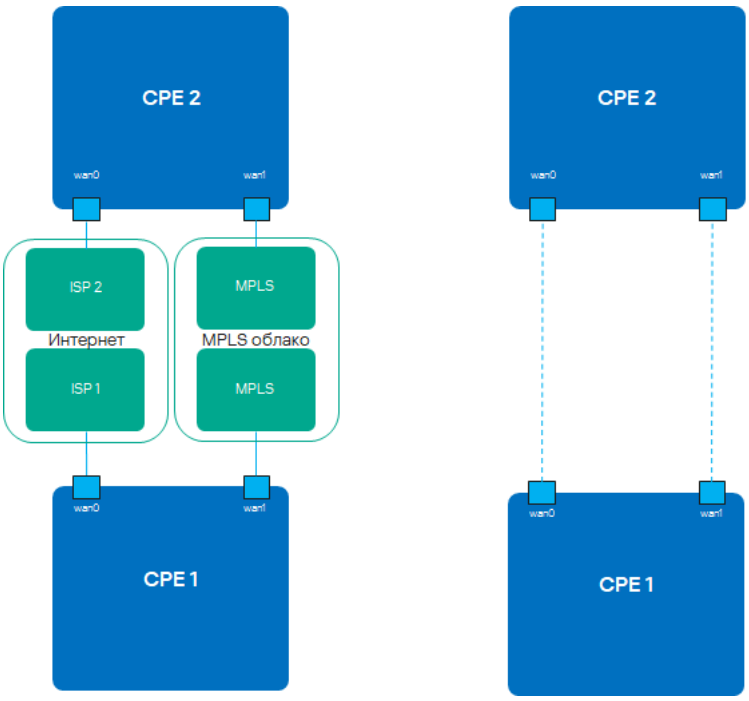
В зависимости от связности устройств CPE через физические каналы передачи данных возможны следующие варианты наложенной связности:

- Все физические каналы передачи данных имеют прямую IP-связность между собой. 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. 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, или 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 следующих подразделах веб-интерфейса оркестратора:

- **Устройства CPE**.
- **Шаблоны CPE**.

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 в том случае, если устройствам CPE не назначено топологических тегов. Такие устройства не пытаются установить прямые туннели между собой, весь трафик в этом случае идет через шлюз SD-WAN.
- **Full-Mesh**. Вам нужно назначить устройствам CPE одинаковый топологический тег для реализации этой топологии. Все устройства с одинаковым топологическим тегом пытаются установить прямые туннели между собой.
- **Partial-Mesh**. Вы можете группировать 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) пытаются установить 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 – это не то же самое, что обычные теги. 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. Если вы назначаете топологический тег отдельному устройству CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.
3. Укажите параметры, определяющие функционирование устройства CPE в топологии:
   - **Роль**.

     Доступные значения:

     - **CPE**. Стандартное устройство. Вы можете добавить это устройство в группу, назначив ему топологический тег.
     - **Gateway**. Шлюз SD-WAN. Вы не можете добавить это устройство в группу.
   - **Транзитное устройство CPE**. Флажок, позволяющий другим устройствам устанавливать туннели через выбранное устройство.

- **Топологические теги**.

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

Качество обслуживания (QoS)

Политика *качества обслуживания* (англ. Quality of Service, далее также QoS) обеспечивает передачу данных в соответствии с требованиями к классам трафика.

В Kaspersky SD-WAN качество обслуживания обеспечивают следующие компоненты:

- **Классы трафика**.

  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**.

  Классификаторы трафика определяют, доверять меткам обслуживания, выставленным в полях заголовков пакетов трафика, или нет. Кроме того, они соотносят трафик с одним из созданных классов.

- **QoS-правила**.

  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**.

    Ограничения 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**.

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**.

  Правила классификации трафика используются для выделения из общего потока данных трафика с определенными значениями полей заголовков уровней L2 – L4, а также трафика определенных 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**.

  Фильтры трафика используются для выполнения следующих задач:

  - обеспечение безопасности путем блокирования избыточного или потенциально опасного трафика;
  - классификация трафика;
  - соблюдение требований SLA для определенных приложений.

  Каждый фильтр состоит из одного или нескольких правил классификации трафика.

QoS на интерфейсах SD-WAN

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 полоска пропускания сначала предлагается трафику из очереди с более высоким приоритетом. Каждой очереди гарантируется минимальная полоса пропускания согласно 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 на пропуск 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 на данный момент Kaspersky SD-WAN не поддерживает создание LAN-интерфейсов SD-WAN, очереди можно настроить только для уже существующих LAN-интерфейсов.

Создание класса трафика

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.

Вы можете создать от 4 до 8 классов трафика при настройке шаблона экземпляра SD-WAN. После того, как с помощью шаблона будет развернут экземпляр SD-WAN, изменить параметры классов трафика или создать новые будет невозможно.

Классы трафика созданные по умолчанию подходят для большинства схем развертывания решения Kaspersky SD-WAN, и мы не рекомендуем изменять их.

Чтобы создать 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 укажите параметры класса трафика:
   - **Имя**.
   - **Очередь**. Номер очереди, в которую требуется помещать трафик класса. Чем выше указанное значение, тем выше приоритет класса трафика. Вы не можете указать одинаковый приоритет для нескольких классов трафика.
   - **KOver**. 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, если общая скорость используется не полностью.
   - **Не учитывать при расчете транспортного пути**. Флажок, позволяющий не учитывать доступную классу трафика скорость при расчете маршрута.

     Если вы установили флажок установлен рядом с классом трафика, вы не можете указать для него коэффициент **KOver**.
   - **Класс трафика по умолчанию**. Класс, в который требуется помещать весь не попавший в другие классы трафик.

- **Класс управляющего трафика**. Класс, в который требуется помещать управляющий трафик.
- **Максимальная зарезервированная скорость (%)**. Процент максимальной скорости передачи, который может быть доступен для одного из созданных классов трафика. Диапазон значений: от 10 до 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

Классификаторы трафика определяют, доверять меткам обслуживания, выставленным в полях заголовков пакетов трафика, или нет. Кроме того, они соотносят трафик с одним из созданных классов. Вы можете создавать классификаторы трафика в следующих разделах/подразделах веб-интерфейса оркестратора:

- **Шаблоны экземпляров SD-WAN**.
- **QoS**.

Чтобы создать классификатор трафика:

1. Откройте список классификаторов трафика одним из следующих способов:
   - В области настройки шаблона экземпляра SD-WAN выберите вкладку **Классификаторы**.
   - В дополнительном меню настройки решения перейдите в раздел **QoS** и выберите вкладку **Классификаторы**.
2. Нажмите на кнопку **+ Добавить классификатор трафика**.
3. В открывшемся окне укажите параметры классификатора трафика:
   - **Имя**.
   - **Типы**.

     Доступные значения:

     - **Trust**. Классификатор, доверяющий меткам обслуживания, выставленным в полях заголовков пакетов трафика. При выборе этого значения в нижней части окна отобразится блок **Сопоставление классов трафика**, в котором вы можете установить соответствие между классами трафика и метками обслуживания.
     - **Untrust**. Классификатор, не доверяющий меткам обслуживания, выставленным в полях заголовков пакетов трафика. При выборе этого значения в нижней части окна отобразится раскрывающийся список **Класс трафика**, в котором вы можете выбрать класс для всего обрабатываемого классификатором трафика.
4. Если в списке **Типы** вы выбрали **Trust**, выполните следующие действия, чтобы установить соответствие между классами трафика и метками обслуживания:
   a. В столбце **Класс трафика** выберите класс для трафика с определенными метками обслуживания.

b. В столбце **Метка обслуживания** нажмите на кнопку **Выбрать** рядом с требуемым заголовком пакета.

c. Установите флажки рядом с метками обслуживания, которые требуется использовать 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.

7. Если вы создали классификатор трафика в подразделе **Шаблоны экземпляров SD-WAN**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона.

Создание QoS-правила

QoS-правила ограничивают скорость передачи трафика, обрабатываемого создаваемыми классификаторами. Вы можете создавать QoS-правила в следующих разделах/подразделах веб-интерфейса оркестратора:

- **Шаблоны экземпляров SD-WAN**.
- **QoS**.

Чтобы создать QoS-правило:

1. Откройте список QoS-правил одним из следующих способов:

   - В области настройки шаблона экземпляра SD-WAN выберите вкладку **QoS-правила**.
   - В дополнительном меню настройки решения перейдите в раздел **QoS** и выберите вкладку **QoS-правила**.

2. Нажмите на кнопку **+ Добавить QoS-правило**.

3. В открывшемся окне укажите параметры QoS-правила:

   - **Имя**.
   - **Классификатор**. Классификатор трафика, который требуется использовать в QoS-правиле.
   - **Без ограничения**. Флажок, позволяющий не ограничивать скорость передачи трафика, обрабатываемого выбранным ранее классификатором.
   - **MBR**. Максимальная скорость передачи трафика (англ. Maximum Bit Rate).
   - **Единицы измерения**. Единицы измерения максимальной скорости передачи трафика.

     Доступные значения:

     - **Кбит/с**.

- **Мбит/с**.
- **Гбит/с**.

- **Максимальная зарезервированная скорость (%)**. Процент от общей скорости передачи трафика, доступный каждому классу. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Классификатор** вы выбрали классификатор трафика с типом Trust. Сумма значений, указанных для каждого класса, должна быть равна 100.

4. Нажмите на кнопку **Применить**.

   QoS-правило отобразится в таблице.

5. Если вы создали классификатор трафика в подразделе **Шаблоны экземпляров SD-WAN**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию шаблона.

Создание ограничения Manual-TE

Ограничения 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.

Перед выполнением этой инструкции требуется создать транспортные пути Manual-TE.

Чтобы создать ограничение Manual-TE:

1. В дополнительном меню настройки решения перейдите в раздел **Ограничения**.
2. Нажмите на кнопку **+ Добавить ограничение Manual-TE**.
3. В открывшемся окне укажите параметры ограничения:
   - **Имя**.
   - **Использовать транспортный путь Manual TE**. Флажок, позволяющий выбрать транспортные пути Manual-TE, которые требуется добавить в ограничение.
   - **Игнорировать, если транспортный путь с ограничением не найден**. Флажок, позволяющий разрешить использование транспортного пути Auto-SPF в случае недоступности Manual-TE.
4. Нажмите на кнопку **Сохранить**.

Ограничение отобразится в таблице. Теперь вы можете указать созданное ограничение в параметрах транспортного сервиса, чтобы добавить в него содержащиеся в ограничении транспортные пути Manual-TE.

Создание порогового ограничения

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.

Перед выполнением этой инструкции требуется включить мониторинг на туннелях.

Чтобы создать пороговое ограничение:

1. В дополнительном меню настройки решения перейдите в раздел **Ограничения** и выберите вкладку **Пороговые ограничения**.
2. Нажмите на кнопку **+ Добавить пороговое ограничение**.
3. В открывшемся окне укажите параметры ограничения:
   - **Имя**.
   - **Не использовать туннели с пороговым значением**. Флажок, позволяющий выбрать показатели мониторинга. Ограничение будет исключать из расчета транспортного пути Auto-TE туннели, на которых достигнуты пороговые значения выбранных показателей мониторинга.
   - **Игнорировать, если транспортный путь с ограничением не найден**. Флажок, позволяющий выбрать показатели мониторинга. Ограничение не исключает из расчета транспортного пути Auto-TE туннели, на которых достигнуты пороговое значения выбранных показателей мониторинга при отсутствии альтернативных туннелей.
4. Нажмите на кнопку **Сохранить**.

Ограничение отобразится в таблице. Теперь вы можете указать созданное ограничение в параметрах транспортного сервиса, чтобы использовать его при автоматическом расчете транспортного пути.

Создание правила классификации трафика

Правила классификации трафика используются для выделения из общего потока данных трафика с определенными значениями полей заголовков уровней L2 – L4, а также трафика определенных 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.

Чтобы создать правило классификации трафика:

1. В дополнительном меню настройки решения перейдите в раздел **Фильтр** и выберите вкладку **Правила**.
2. Вверху справа нажмите на кнопку **+ Добавить правило**.
3. В открывшемся окне укажите параметры правила классификации трафика:
   - **Имя**.

- **L2-поля**, **L3-поля**, **L4-поля**. Вкладки, на которых отображаются поля заголовков пакетов трафика уровней L2 – L4, с помощью которых правило выделяет определенный трафик из общего пакета данных. Вы можете установить флажки рядом с полями, после чего указать для них требуемые значения.

4. Если требуется, выполните следующие действия, чтобы выбрать приложение, трафик которого правило должно выделять из общего потока данных:

   a. Выберите вкладку **DPI**.

   b. Установите флажок **Метка PKT**.

   c. Установите флажок **Приложение** и в раскрывающемся списке справа выберите приложение.

5. Нажмите на кнопку **Создать**.

Правило классификации трафика отобразится в таблице. Теперь вы можете использовать его при создании фильтра трафика.

Создание фильтра трафика

Фильтры трафика используются для выполнения следующих задач:

- обеспечение безопасности путем блокирования избыточного или потенциально опасного трафика;
- классификация трафика;
- соблюдение требований SLA для определенных приложений.

Каждый фильтр состоит из одного или нескольких правил классификации трафика.

Перед выполнением этой инструкции требуется создать как минимум одно правило классификации трафика.

Чтобы создать фильтр трафика:

1. В дополнительном меню настройки решения перейдите в раздел **Фильтр**.
2. Вверху справа нажмите на кнопку **+ Добавить фильтр**.
3. В открывшемся окне укажите параметры фильтра трафика:

   - **Имя**.
   - **Порядковый номер**. Правило классификации трафика с наименьшим значением порядкового номера обрабатывается первым. Диапазон значений: от 1 до 998.
   - **Правило**. Правило классификации трафика, которое требуется добавить в фильтр.
   - **Действие**. Действие, которое правило классификации трафика должно применять к выделяемому из общего потока данных трафику.

     Доступные значения:

     - **Permit**. Разрешить дальнейшую маршрутизацию трафика.

- **Deny**. Запретить дальнейшую маршрутизацию трафика.

4. Нажмите на кнопку **Добавить**, чтобы добавить правило классификации трафика в фильтр.
5. В раскрывающемся списке **Действие по умолчанию (Посл=999**) выберите действие, которое требуется применять ко всему остальному трафику:
   - **Permit**.
   - **Deny**.
6. Нажмите на кнопку **Сохранить**.

Фильтр трафика отобразится в таблице. Теперь вы можете использовать его при создании транспортных сервисов.

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**.

  Транспортный сервис P2P (E-line в классификации MEF) используется для передачи трафика между двумя сервисными интерфейсами устройств CPE. В рамках этого транспортного сервиса первый сервисный интерфейс является источником (англ. source), а второй – назначением (англ. destination).

  Для сервисного интерфейса-источника можно добавить резервный (англ. backup) сервисный интерфейс. При этом резервный сервисный интерфейс может быть добавлен на том же самом или любом другом устройстве CPE.

  Поддерживается передача кадров, соответствующих стандартам IEEE 802.1Q и 802.1AD.

- **P2M**.

Транспортный сервис P2M (E-tree в классификации MEF) 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.

Для каждого сервисного интерфейса можно добавить резервный сервисный интерфейс. При этом резервный сервисный интерфейс может быть добавлен на том же самом или любом другом устройстве CPE.

Поддерживается передача кадров, соответствующих стандартам IEEE 802.1Q и 802.1AD.

- M2M.

Транспортный сервис M2M (E-LAN в классификации MEF) 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.

Для каждого сервисного интерфейса можно добавить резервный сервисный интерфейс. При этом резервный сервисный интерфейс может быть добавлен на том же самом или любом другом устройстве CPE.

- IP multicast.

Транспортный сервис IP multicast 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 сервисный интерфейс-источник).

Сервисный интерфейс-источник передает multicast-трафик на сервисные интерфейсы, к которым подключены подписчики (далее также сервисные интерфейсы-подписчики). Сервисные 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.

Транспортный сервис L3 VPN 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.

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

Транспортный сервис P2P (E-line в классификации MEF) используется для передачи трафика между двумя сервисными интерфейсами устройств CPE. В рамках этого транспортного сервиса первый сервисный интерфейс является источником (англ. source), а второй – назначением (англ. destination).

Для сервисного интерфейса-источника можно добавить резервный (англ. backup) сервисный интерфейс. При этом резервный сервисный интерфейс может быть добавлен на том же самом или любом другом устройстве CPE.

Поддерживается передача кадров, соответствующих стандартам IEEE 802.1Q и 802.1AD.

Перед выполнением этой инструкции требуется выполнить следующие действия:

- активировать устройства CPE;
- создать сервисные интерфейсы.

Чтобы создать транспортный сервис P2P:

1. В дополнительном меню настройки решения перейдите в раздел **P2P**.
2. Нажмите на кнопку **+ Добавить P2P**.
3. В открывшемся окне укажите параметры транспортного сервиса P2P:
   - **Имя**.
   - **Ограничение**. Параметр, позволяющий добавить ограничение (Manual-TE или пороговое) в транспортный сервис.
   - **Режим балансировки**.

     Доступные значения:

     - **Per-flow**. Балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям.
     - **Per-packet**. Балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.

- **Broadcast**. Пакеты передаются одновременно во все туннели для исключения потерь.

- **Описание**.

- **Коммутатор** и **Порт**. Параметры, позволяющие выбрать сервисный интерфейс-источника и сервисный интерфейс-назначения.

- **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.

- **Переключить сервисные интерфейсы**. Флажок, позволяющий, поменять местами значения, выбранные в раскрывающемся списке **Порт** для сервисного интерфейса-источника и -назначения.

- **Резервный сервисный интерфейс**. Флажок, позволяющий добавить резервный сервисный интерфейс-источник.

  Если флажок установлен, укажите параметры резервного сервисного интерфейса:

  - **Резервный коммутатор** и **Резервный порт**. Параметры, позволяющие выбрать резервный сервисный интерфейс.

  - **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Резервный порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.

  > Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.

- **Входящий фильтр**. Фильтр трафика для сервисных интерфейсов.

- **QoS**. Правило качества обслуживания для сервисного интерфейса-источника.

- **Транслировать статус интерфейса**. Флажок, позволяющий отслеживать состояние обоих сервисных интерфейсов, и при выключении одного из них автоматически выключать второй.

  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.

  Флажок невозможно установить, если установлен флажок **Резервный сервисный интерфейс**.

4. Нажмите на кнопку **Сохранить**.

Транспортный сервис P2P отобразится в таблице.

Создание P2M

Транспортный сервис P2M (E-tree в классификации MEF) 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.

Для каждого сервисного интерфейса можно добавить резервный сервисный интерфейс. При этом резервный сервисный интерфейс может быть добавлен на том же самом или любом другом устройстве CPE.

Поддерживается передача кадров, соответствующих стандартам IEEE 802.1Q и 802.1AD.

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 решения перейдите в раздел **P2M**.
2. Нажмите на кнопку **+ Добавить P2M**.
3. В открывшемся окне укажите параметры транспортного сервиса P2M:
   - **Имя**.
   - **Ограничение**. Параметр, позволяющий добавить ограничение (Manual-TE или пороговое) в транспортный сервис.
   - **Режим балансировки**.

     Доступные значения:

     - **Per-flow**. Балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям.
     - **Per-packet**. Балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
     - **Broadcast**. Пакеты передаются одновременно во все туннели для исключения потерь.
   - **Режим изучения MAC**. 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.

     Доступные значения:

     - **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 она пришла изначально.
     - **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.

- **Время жизни MAC, сек**. Время в секундах, в течение которого записи хранятся в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 10 до 65535.
- **При переполнении MAC-таблицы**. Политика обработки новых MAC-адресов при переполнении MAC-таблицы на контроллере SD-WAN.

  Доступные значения:

  - **flood**. Трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast).
  - **drop**. Трафик с ранее неизученными MAC-адресами назначения не передается.
- **Размер таблицы MAC-адресов**. 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.
- **Режим работы транспортного сервиса**. Параметр, позволяющий использовать или не 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:

  - **Classic**. Не использовать DFI.
  - **DFI with FIB on ROOT and LEAF**. 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 with FIB on 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.
- **Описание**.

4. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

5. Укажите параметры сервисного интерфейса:

   - **Коммутатор** и **Порт**. Параметры, позволяющие выбрать сервисный интерфейс.
   - **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.
   - **QoS**. Правило качества обслуживания для сервисного интерфейса.
   - **Входящий фильтр**. Фильтр трафика для сервисного интерфейса.
   - **Роль**. Роль сервисного интерфейса.

     Доступные значения:

- **LEAF**.
- **ROOT**.

- **Резервный сервисный интерфейс**. Флажок, позволяющий добавить резервный сервисный интерфейс.

  Если флажок установлен, укажите параметры резервного сервисного интерфейса:

  - **Резервный коммутатор** и **Резервный порт**. Параметры, позволяющие выбрать резервный сервисный интерфейс.
  - **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Резервный порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.

  > Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.

- **Default forwarding interface**. Флажок, позволяющий назначить роль DFI сервисному интерфейсу.

6. Нажмите на кнопку **+ Добавить**, чтобы добавить сервисный интерфейс в транспортный сервис.

   Сервисный интерфейс отобразится в нижней части окна.

7. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

8. Укажите параметры OpenFlow-интерфейсов:

   - **Группа**. Группа OpenFlow-интерфейсов, которую требуется добавить. Поверх каждого OpenFlow-интерфейса в группе автоматически создается сервисный интерфейс, который в свою очередь добавляется в транспортный сервис.
   - **QoS**. Правило качества обслуживания для сервисных интерфейсов, созданных поверх OpenFlow-интерфейсов.
   - **VLAN ID**. 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.
   - **Роль**. Роль для сервисных интерфейсов, автоматически созданных поверх OpenFlow-интерфейсов.

     Доступные значения:

     - **LEAF**.
     - **ROOT**.

9. Нажмите на кнопку **+ Добавить**, чтобы добавить группу OpenFlow-интерфейсов в транспортный сервис.

   Автоматически созданные сервисные интерфейсы отобразятся в нижней части окна.

10. Нажмите на кнопку **Сохранить**.

Транспортный сервис P2M отобразится в таблице.

Создание M2M

Транспортный сервис M2M (E-LAN в классификации MEF) 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.

Для каждого сервисного интерфейса можно добавить резервный сервисный интерфейс. При этом резервный сервисный интерфейс может быть добавлен на том же самом или любом другом устройстве CPE.

Перед выполнением этой инструкции требуется выполнить следующие действия:

- активировать устройства CPE;
- создать сервисные интерфейсы.

Чтобы создать транспортный сервис M2M:

1. В дополнительном меню настройки решения перейдите в раздел **M2M**.
2. Нажмите на кнопку **+ Добавить M2M**.
3. В открывшемся окне укажите параметры транспортного сервиса M2M:
   - **Имя**.
   - **Ограничение**. Параметр, позволяющий добавить ограничение (Manual-TE или пороговое) в транспортный сервис.
   - **Режим балансировки**.

     Доступные значения:

     - **Per-flow**. Балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям.
     - **Per-packet**. Балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
     - **Broadcast**. Пакеты передаются одновременно во все туннели для исключения потерь.
   - **Режим изучения MAC**. 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.

     Доступные значения:

     - **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 она пришла изначально.

- **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.

- **Время жизни MAC, сек**. Время в секундах, в течение которого записи хранятся в MAC-таблице на контроллере SD-WAN. Диапазон значений: от 10 до 65535.
- **При переполнении MAC-таблицы**. Политика обработки новых MAC-адресов при переполнении MAC-таблицы на контроллере SD-WAN.

  Доступные значения:

  - **flood**. Трафик с ранее неизученными MAC-адресами назначения передается как BUM-трафик (Broadcast, unknown-unicast, and multicast).
  - **drop**. Трафик с ранее неизученными MAC-адресами назначения не передается.

- **Размер таблицы MAC-адресов**. 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.
- **Описание**.

4. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.
5. Укажите параметры сервисного интерфейса:
   - **Коммутатор** и **Порт**. Параметры, позволяющие выбрать сервисный интерфейс.
   - **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.
   - **QoS**. Правило качества обслуживания для сервисного интерфейса.
   - **Входящий фильтр**. Фильтр трафика для сервисного интерфейса.
   - **Резервный сервисный интерфейс**. Флажок, позволяющий добавить резервный сервисный интерфейс.

     Если флажок установлен, укажите параметры резервного сервисного интерфейса:

     - **Резервный коммутатор** и **Резервный порт**. Параметры, позволяющие выбрать резервный сервисный интерфейс.
     - **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Резервный порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.

   > 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.

7. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

8. Укажите параметры OpenFlow-интерфейсов:

   - **Группа**. Группа OpenFlow-интерфейсов, которую требуется добавить. Поверх каждого OpenFlow-интерфейса в группе автоматически создается сервисный интерфейс, который в свою очередь добавляется в транспортный сервис.

   - **QoS**. Правило качества обслуживания для сервисных интерфейсов, созданных поверх OpenFlow-интерфейсов.

   - **VLAN ID**. 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.

10. Нажмите на кнопку **Сохранить**.

Транспортный сервис M2M отобразится в таблице.

Создание IP multicast

Транспортный сервис IP multicast 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 сервисный интерфейс-источник).

Сервисный интерфейс-источник передает multicast-трафик на сервисные интерфейсы, к которым подключены подписчики (далее также сервисные интерфейсы-подписчики). Сервисные 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.

Для каждого сервисного интерфейса-источника можно добавить резервный сервисный интерфейс. При этом резервный сервисный интерфейс может быть создан на том же самом или любом другом устройстве CPE.

Использование транспортного сервиса IP multicast обеспечивает сохранение полосы пропускания трафика, что в свою очередь снижает объем передаваемого трафика за счет одновременной доставки одного и того же потока информации нескольким подписчикам при групповой передаче.

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 решения перейдите в раздел **IP multicast**.
2. Нажмите на кнопку **+ Добавить IP multicast**.
3. В открывшемся окне укажите параметры транспортного сервиса IP multicast:
   - **Имя**.
   - **Основной коммутатор** и **Основной порт**. Параметры, позволяющие выбрать сервисный интерфейс-источник.
   - **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Основной порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.
   - **IP источника**. IP-адрес сервисного интерфейса-источника.
   - **Резервный сервисный интерфейс**. Флажок, позволяющий добавить резервный сервисный интерфейс-источник.

     Если флажок установлен, укажите параметры резервного сервисного интерфейса:

     - **Резервный коммутатор** и **Резервный порт**. Параметры, позволяющие выбрать резервный сервисный интерфейс.
     - **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Резервный порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.

       Если основной сервисный интерфейс возобновляет работу, транспортный сервис продолжает использовать резервный сервисный интерфейс.
   - **Переключаться на основной сервисный интерфейс**. Флажок, позволяющий прекращать использование резервного сервисного интерфейса в случае восстановления основного. Этот флажок можно установить только если вы добавили резервный сервисный интерфейс-источник.
   - **Резервное multicast-дерево**. Флажок, позволяющий 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.

     Флажок может быть установлен только если вы добавили резервный сервисный интерфейс-источник.
   - **IGMP-прокси**. Флажок, позволяющий использовать прокси-сервер IGMP. Эта функция сохраняет передачу трафика на активные multicast-группы, к которым подключен как минимум один сервисный интерфейс-подписчик.
   - **QoS**. Правило качества обслуживания для сервисного интерфейса-источника.
4. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.
5. Укажите параметры сервисного интерфейса-подписчика:
   - **Коммутатор** и **Порт**. Параметры, позволяющие выбрать сервисный интерфейс-подписчик.
   - **Показать используемые сервисные интерфейсы**. Флажок, позволяющий выбрать в раскрывающемся списке **Порт** сервисный интерфейс, который ранее был добавлен в транспортные сервисы.
6. Нажмите на кнопку **+ Добавить**, чтобы добавить сервисный интерфейс в транспортный сервис.

Сервисный интерфейс отобразится в нижней части окна.

7. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.
8. Укажите параметры multicast-группы:
   - **IP-адрес**. Диапазон значений: от 224.0.0.0 до 239.255.255.255.
   - **Маска**. Маска IP-адреса. Диапазон значений: от 24 до 32.
   - **GBR**. Гарантированная 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.
10. Нажмите на кнопку **Сохранить**.

Транспортный сервис IP multicast отобразится в таблице.

Создание L3 VPN

Транспортный сервис L3 VPN 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.

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 решения перейдите в раздел **L3 VPN**.
2. Нажмите на кнопку **+ Добавить L3 VPN**.
3. В открывшемся окне укажите параметры транспортного сервиса L3 VPN:
   - **Имя**.
   - **Ограничение**. Параметр, позволяющий добавить ограничение (Manual-TE или пороговое) в транспортный сервис.
   - **Режим балансировки**.
     Доступные значения:
     - **Per-flow**. Балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям.

- **Per-packet**. Балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
- **Broadcast**. Пакеты передаются одновременно во все туннели для исключения потерь.

4. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

5. Укажите параметры L3-интерфейса:

   - **Режим**. Тип L3-интерфейса.

     Доступные значения:

     - **M2M Point**. Создать L3-интерфейс поверх транспортного сервиса M2M. При выборе этого значения становится доступным список **Сеть**. Поверх выбранного в этом списке транспортного сервиса M2M создается L3-интерфейс.
     - **Switch/port point**. Создать L3-интерфейс поверх сервисного интерфейса.

     Если в раскрывающемся списке **Режим** вы выбрали **Switch/port point**, укажите параметры сервисного интерфейса:

     - **Коммутатор** и **Сервисный интерфейс**. Параметры, позволяющие выбрать сервисный интерфейс.
     - **VLAN по умолчанию**. Внешняя VLAN-метка.
     - **QoS**. Правило качества обслуживания для сервисного интерфейса.
     - **Входящий фильтр**. Фильтр трафика для сервисного интерфейса.

   - **IP**. IP-адрес L3-интерфейса.
   - **Длина префикса**. Длина префикса L3-интерфейса. Диапазон значений: от 0 до 32.
   - **MAC**. MAC-адрес сервисного интерфейса. Вы можете ввести MAC-адрес вручную либо нажать на кнопку **Сгенерировать**, чтобы сгенерировать MAC-адрес.
   - **Время жизни (сек.)**. Время в секундах, в течение которого могут храниться в ARP-таблице на контроллере SD-WAN. Диапазон значений: от 1 до 65535.
   - **Включить DHCP Relay**. Флажок, позволяющий перенаправлять запрос `DHCPDISCOVER` на сервер или серверы, которые вы сможете указать позже в блоке **Серверы DHCP**.

6. Нажмите на кнопку **+ Добавить**, чтобы создать L3-интерфейс.

   L3-интерфейс отобразится в нижней части окна.

7. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

8. Укажите параметры статического маршрута:

   - **IP**. IP-адрес узла или сети назначения.
   - **Длина префикса**. Длина префикса узла назначения. Диапазон значений: от 0 до 32.
   - **SVI**. L3-интерфейс для отправки пакетов трафика на узел назначения.
   - **Шлюз**. IP-адрес шлюза для маршрутизации пакетов трафика.

- **Метрика**. Метрика статического маршрута.

9. Нажмите на кнопку **+ Добавить**, чтобы создать статический маршрут.

   Статический маршрут отобразится в нижней части окна.

10. Нажмите на кнопку **Далее** для перехода к следующей группе параметров.

11. Если требуется, в блоке **Серверы DHCP** нажмите на кнопку **+ Добавить** и введите IP-адрес DHCP-сервера, чтобы добавить его в транспортный сервис.

12. Нажмите на кнопку **Сохранить**.

Транспортный сервис L3 VPN отобразится в таблице.

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. При добавлении транспортного сервиса в шаблон CPE требуется указать те же параметры, которые вы указали при его изначальном создании. Например, вам нужно использовать то же самое имя и тип.

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. Укажите параметры транспортного сервиса:

   - **Имя**.

   - **Имя QoS**. Имя правила качества обслуживания, которое используется в транспортном сервисе.

   - **Стадия**. Состояние устройства CPE, в котором сервисный интерфейс требуется добавить в транспортный сервис.

     Доступные значения:

     - **Перед активацией**. Сервисный интерфейс добавляется в транспортный сервис перед активацией устройства CPE.

     - **После активации**. Сервисный интерфейс добавляется в транспортный сервис после активации устройства CPE.

   - **Тип транспортного сервиса**.

     Доступные значения:

- **P2M**.
- **M2M**.
- **L3VPN**.

- **Роль**. Роль сервисного интерфейса. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Тип транспортного сервиса** вы выбрали **P2M**.

  Доступные значения

  - **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.

- **IP-адрес** и **Маска**. IP-адрес и маска интерфейса транспортного сервиса. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Тип транспортного сервиса** вы выбрали **L3VPN**.

- **Инкапсуляция**. Тип инкапсуляции на сервисном интерфейсе.

  Доступные значения:

  - **Access**.
  - **VLAN**.
  - **Q-in-Q**.

- **VLAN ID**. Внешняя метка VLAN. Диапазон значений: от 1 до 4094. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Инкапсуляция** вы выбрали **VLAN** или **Q-in-Q**.

- **Внутренний VLAN ID**. Внутренняя метка VLAN. Диапазон значений: от 1 до 4094. Вы можете указать значение для этого параметра только если в раскрывающемся списке **Инкапсуляция** вы выбрали **Q-in-Q**.

4. Нажмите на кнопку **Сохранить**.

   Транспортный сервис отобразится в таблице.

5. 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 решения 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 укажите параметры статической записи:

   - **Коммутатор** и **Сервисный интерфейс**. Параметры, позволяющие назначить соответствие между IP и MAC-адресом сервисного интерфейса.
   - **IP-адрес**. IP-адрес сервисного интерфейса.
   - **MAC**. MAC-адрес сервисного интерфейса.

5. Нажмите на кнопку **Сохранить**.

Статическая запись отобразится в ARP-таблице. Вы можете в дальнейшем изменить или удалить запись с помощью соответствующих действий, доступных по кнопке **Управление** в строке ARP-записи.

Просмотр MAC-таблицы транспортных сервисов P2M и M2M

Вы можете просмотреть MAC-таблицу транспортных сервисов P2P и M2M.

Чтобы просмотреть MAC-таблицу транспортного сервиса:

1. В дополнительном меню настройки решения перейдите в раздел **P2M** или **M2M**.
2. Нажмите на кнопку **Управление** рядом с требуемым транспортным сервисом и в раскрывающемся списке выберите **Таблица MAC-адресов**.

Просмотр таблицы маршрутизации транспортного сервиса L3 VPN

Чтобы просмотреть таблицу маршрутизации транспортного сервиса L3 VPN:

1. В дополнительном меню настройки решения перейдите в раздел **L3 VPN**.
2. Нажмите на кнопку **Управление** рядом требуемым транспортным сервисом и в раскрывающемся списке выберите **Таблица маршрутизации**.

Просмотр статистики работы транспортного сервиса

Вы можете просмотреть статистику работы транспортных сервисов P2P, P2M, M2M и IP multicast.

Чтобы просмотреть статистику работы транспортного сервиса:

1. В дополнительном меню настройки решения перейдите в один из следующих разделов:

   - **P2P**.
   - **P2M**.
   - **M2M**.
   - **IP multicast**.

2. Нажмите на кнопку **Управление** рядом с требуемым транспортным сервисом, и в раскрывающемся списке выберите **Статистика**.

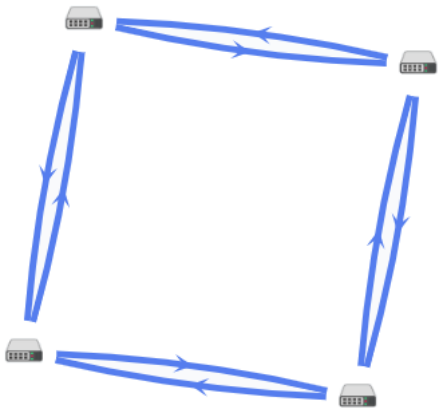
Просмотр топологии транспортного сервиса

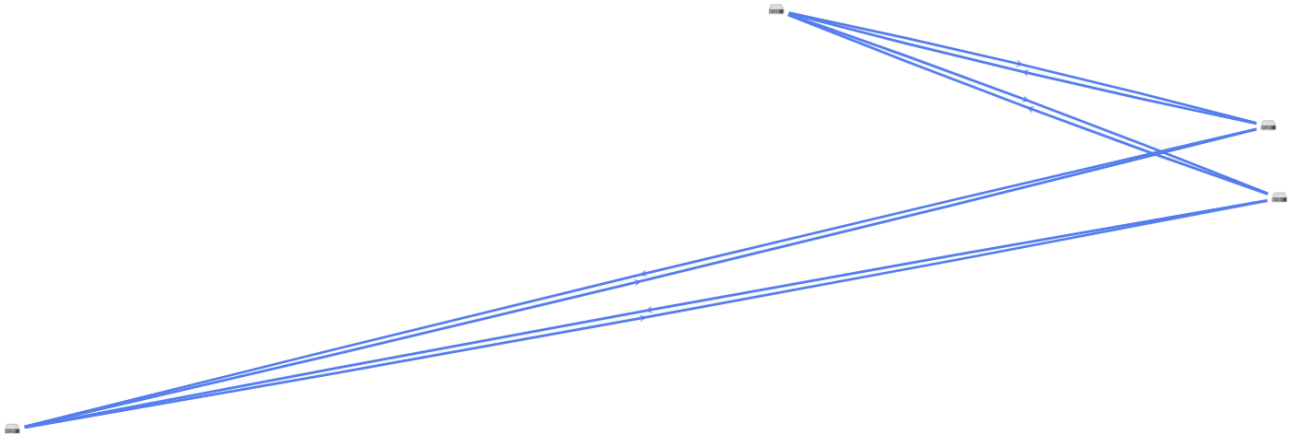
Вы можете просмотреть топологию транспортных сервисов P2P, P2M и M2M.

Чтобы просмотреть топологию транспортного сервиса:

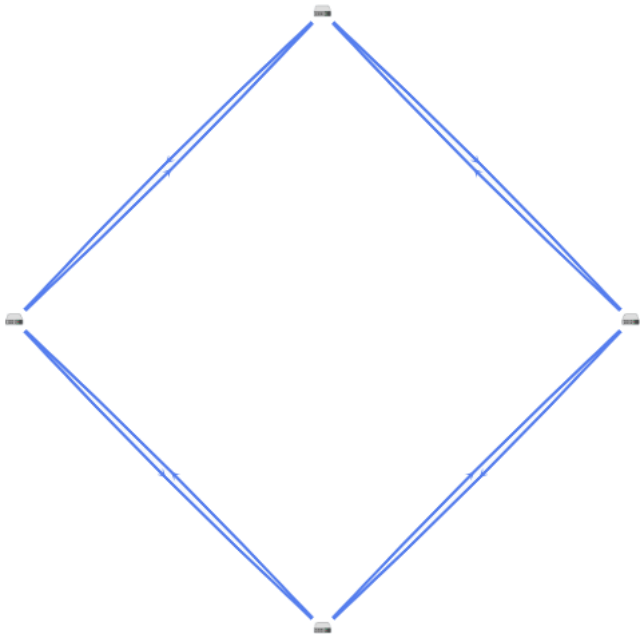
1. В дополнительном меню настройки решения перейдите в один из следующих разделов:
   - **P2P**.
   - **P2M**.
   - **M2M**.
2. Нажмите на кнопку **Управление** рядом с требуемым транспортным сервисом и в раскрывающемся списке выберите **Топология**.

   Откроется окно с топологией транспортного сервиса.
3. Если необходимо изменить взаимное расположение устройств CPE, используйте кнопки справа вверху:
   - **Вручную**. Вы можете вручную изменять 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:

       
     - **Случайно**. Устройства CPE располагаются случайным образом. Например:

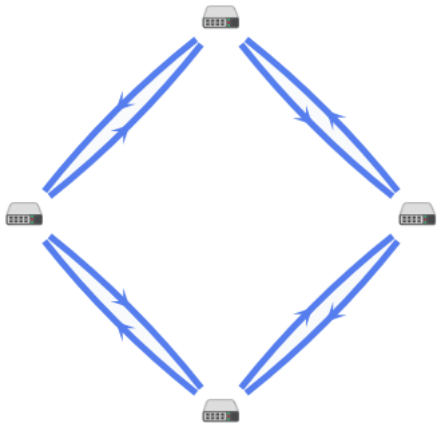


Кольцо. Устройства CPE располагаются в соответствии с топологией кольцо. Например:



- **Горизонтально**. Устройства CPE располагаются горизонтально (в ширину). Например:

Концентрически. Устройства CPE располагаются концентрически. Например:



Решетка. Устройства CPE располагаются в соответствии с топологией решетка. Например:

4. Для отображения подписей к устройствам установите следующие флажки:

- **Имя**.
- **IP-адрес**.

5. Для отображения туннелей, используемых в сегменте из двух устройств CPE, установите флажок **Сегменты** и выберите требуемые устройства в раскрывающихся списках снизу или на схеме.

6. Для получения дополнительной информации об устройстве CPE или туннеле, а также для доступа к элементам управления ими, нажмите на значок устройства или туннеля.

Обновление, изменение и удаление транспортного сервиса

Чтобы обновить, изменить или удалить транспортный сервис:

1. В дополнительном меню настройки решения перейдите в один из следующих разделов:

   - **P2P**.
   - **P2M**.
   - **M2M**.
   - **IP multicast**.
   - **L3 VPN**.

2. Нажмите на кнопку **Управление** рядом с требуемым транспортным сервисом, и выберите нужное действие:

   - Для обновления транспортного сервиса выберите **Повторная инициализация**.

     Откроется окно с сообщением об успешном перезапуске транспортного сервиса. При успешном обновлении транспортного сервиса контроллер SD-WAN снова добавляет его на всех устройствах CPE, которые в нем использовались.

   - Для изменения параметров транспортного сервиса выберите **Изменить**. Информацию о параметрах транспортных сервисов вы найдете в инструкциях по созданию P2P, P2M, M2M, IP multicast и L3 VPN.

   - Для удаления транспортного сервиса выберите **Удалить**. Если нужно также удалить добавленные в транспортный сервис сервисные интерфейсы, в окне подтверждения установите флажок **Удалить используемые сервисные интерфейсы**.

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 выделения трафика определенного 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 него будет поступать трафик приложения.

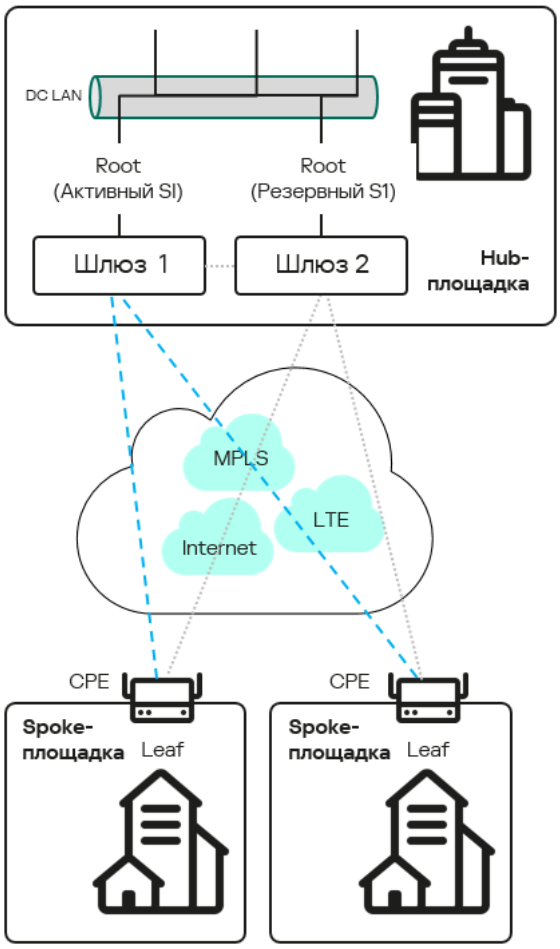
Примеры топологий Hub-and-Spoke

Топология Hub-and-Spoke является наиболее распространенной при построении сетей SD-WAN. 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.

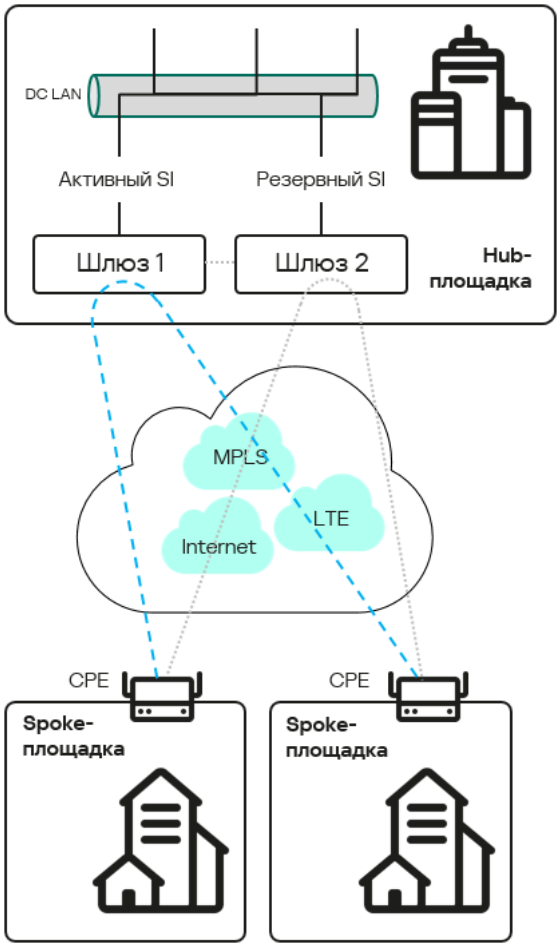


Вам нужно создать транспортный сервис P2M, чтобы построить такую топологию. В качестве точек назначения требуется использовать сервисные интерфейсы на шлюзах SD-WAN 1 и 2 и назначить им роль Root.

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.



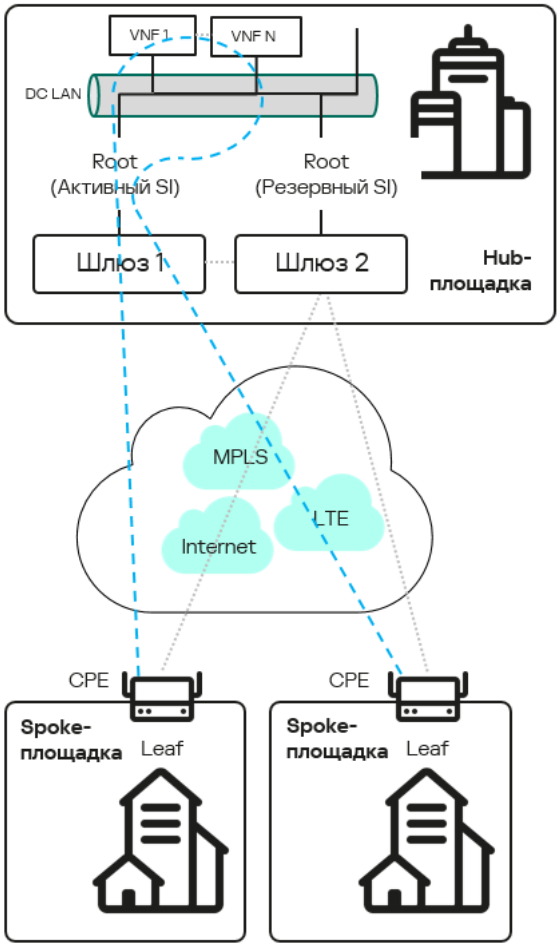
Вам нужно создать транспортный сервис P2M или M2M, чтобы построить такую топологию. В качестве точек назначения требуется использовать сервисные интерфейсы на шлюзах SD-WAN 1 и 2. При использовании транспортного сервиса P2M сервисным интерфейсам требуется назначить роль Root.

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).



Вам нужно создать транспортный сервис P2M, чтобы построить такую топологию, после чего убедиться, что сетевой сервис SD-WAN, развернутый для тенанта, содержит в цепочке все требуемые VNF.

Основные функции

Kaspersky SD-WAN поддерживает большое количество функций, которые упрощают работу с **устройствами CPE** и передачу трафика между ними, повышают общую доступность решения и делают его работу более безопасной, а также обеспечивают мониторинг его компонентов. В этом разделе содержится описание этих функций.

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.

Указание стоимости туннеля

Вы можете указывать стоимость туннелей в следующих разделах/подразделах веб-интерфейса оркестратора:

- **Устройства CPE**.
- **Топология**.
- **Туннели**.

Чтобы указать стоимость туннеля:

1. Откройте окно настройки стоимости туннеля одним из следующих способов:
   - 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**.
   - В дополнительном меню настройки решения 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 решения перейдите в раздел **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**. Это даст возможность указывать стоимость отдельно на туннеле.
3. Укажите требуемые параметры:
   - **Стоимость**.
   - **Для обоих туннелей**. Флажок, позволяющий автоматически назначить указанную стоимость аналогичному встречному туннелю.
4. Нажмите на кнопку **Сохранить**.
5. Если вы указали стоимость туннеля в разделе **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.

Функция Dampening позволяет выполнять 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 следующих разделах/подразделах веб-интерфейса оркестратора:

- **Устройства CPE**.
- **Топология**.
- **Туннели**.

По умолчанию функция выключена на туннелях.

Чтобы включить функцию Dampening на туннеле:

1. Откройте окно настройки функции Dampening одним из следующих способов:

   - 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**.

   - В дополнительном меню настройки решения 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 решения перейдите в раздел **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 укажите параметры функции Dampening:

   - **Максимальное время блокировки (мс)**. Максимальное время в миллисекундах, в течение которого доступ к туннелю может быть ограничен. По истечении указанного времени все счетчики функции Dampening на туннеле сбрасываются.

   - **Штраф**. Число, которое требуется прибавлять к показателю Penalty при изменении состояния туннеля.

   - **Порог блокировки**. Значение показателя Penalty, при котором доступ к туннелю ограничивается.

   - **Интервал обновления (мс)**. Время в миллисекундах, за которое показатель Penalty должен набрать значение, указанное в поле **Порог блокировки**, для ограничения доступа к туннелю.

3. Если требуется, нажмите на кнопку **Загрузить статистику**, чтобы отобразить показатели работы функции Dampening на туннеле.

4. 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.

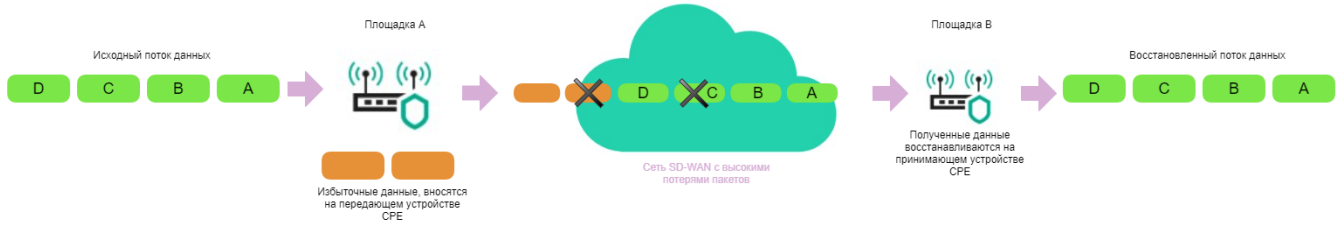


Схема работы функции FEC

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.

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.

Мы рекомендуем использовать FEC на так называемых noisy links (или зашумленных туннелях) для уменьшения коэффициента потери пакетов трафика и увеличения скорости TCP-соединений.

Вы можете включить функцию FEC на туннелях в следующих разделах/подразделах веб-интерфейса оркестратора:

- **Устройства CPE**.
- **Топология**.
- **Туннели**.

По умолчанию функция выключена на туннелях.

Чтобы включить функцию FEC на туннеле:

1. Откройте окно настройки функции FEC одним из следующих способов:

   - 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**.
   - В дополнительном меню настройки решения 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 решения 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**.

2. В открывшемся окне установите флажок **Переопределить**. Это даст возможность настраивать FEC отдельно на туннеле.

3. Укажите параметры FEC:

   - **Степень избыточности, исходные/дополнительные пакеты**. Степень избыточности передаваемых пакетов трафика, которая является соотношением между оригинальными пакетами и дополнительными пакетами, содержащими избыточный код. При выборе значения **0:0 FEC off** функция не используется.

   - **Тайм-аут**. Максимальное время в миллисекундах, в течение которого пакет трафика может находиться в очереди для применения функции FEC. Диапазон значений: от 1 до 1000.

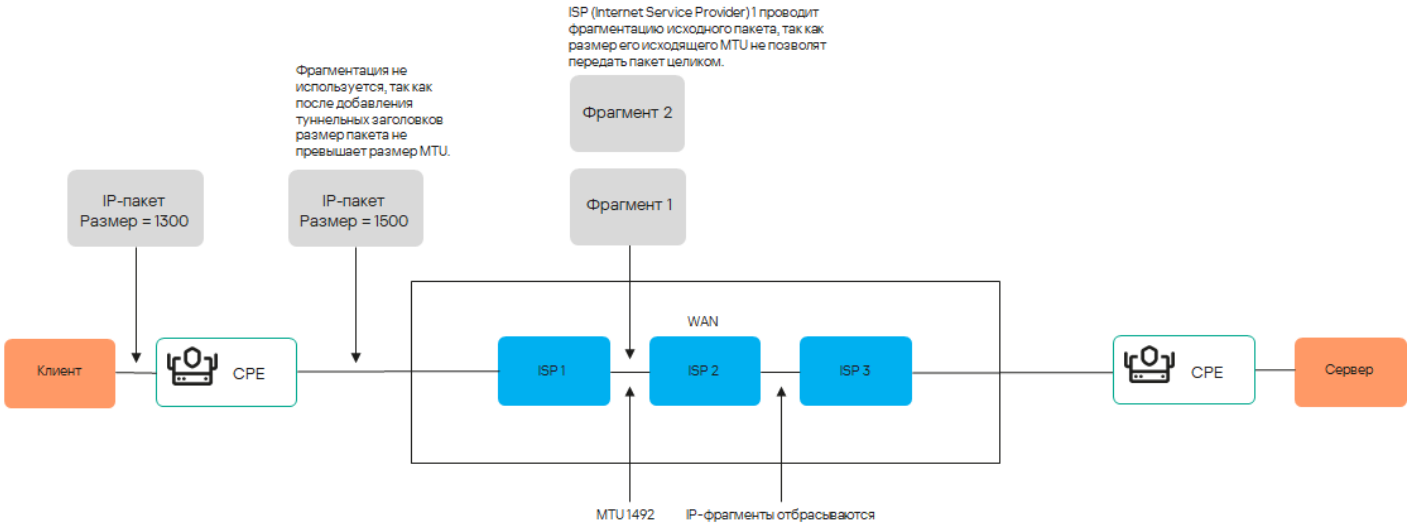
4. Нажмите на кнопку **Сохранить**.

5. Если вы включили функцию FEC на туннеле в подразделе **Устройства CPE**, вверху справа нажмите на кнопку **Сохранить**, чтобы сохранить конфигурацию устройства.

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 параметре `topology.link.pmtud.scheduler.interval.sec` контроллера SD-WAN. По умолчанию задана периодичность 86400 секунд.

- Вручную по запросу в веб-интерфейсе оркестратора. Вы можете отправить запрос на вычисление MTU на туннеле в следующих разделах/подразделах:

- **Устройства CPE**.
- **Туннели**.

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 одним из следующих способов:
   - В дополнительном меню настройки решения 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 параметра `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 включать или выключать 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. Если вы включаете или выключаете шифрование трафика на отдельном устройстве CPE, установите флажок **Переопределить**. Это даст возможность изменить параметры, унаследованные из шаблона CPE.

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 включать и выключать шифрование трафика на отдельных туннелях в следующих разделах/подразделах веб-интерфейса оркестратора:

- **Устройства CPE**.
- **Топология**.
- **Туннели**.

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 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 трафика**.

   - В дополнительном меню настройки решения перейдите в раздел **Топология**, нажмите на туннель, на котором требуется включить или выключить шифрование трафика, и в открывшемся окне нажмите на кнопку **Включить шифрование трафика**.

   - В дополнительном меню настройки решения 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 трафика**.

2. В открывшемся окне установите флажок **Переопределить**. Это даст возможность включать и выключать шифрование трафика отдельно на туннеле.

3. Установите или снимите флажок **Включить шифрование трафика**.

4. 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 на данный момент не поддерживается 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 решения перейдите в раздел **TAP**.
2. Нажмите на кнопку **+ Добавить точку назначения**.
3. В открывшемся окне с помощью раскрывающихся списков **Коммутатор** и **Порт** выберите сервисный интерфейс, который требуется использовать в качестве точки назначения трафика.
4. Нажмите на кнопку **Создать**.

Точка назначения трафика отобразится в таблице.

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 решения перейдите в раздел **TAP**.
2. Выберите вкладку **TAP**.
3. Нажмите на кнопку **+ Добавить TAP**.
4. В открывшемся окне укажите параметры TAP-сервиса:

- **Зеркалировать**. Флажок, позволяющий зеркалировать на точку назначения трафик, поступающий в точки сбора. При зеркалировании на точку назначения передается копия трафика.

  Если флажок не установлен, трафик перенаправляется.

- **Режим балансировки**. Режим балансировки для TAP-сервиса.

  Доступные значения:

  - **Per-flow**. Балансировка по потокам (сессиям). При передаче потоки распределяются равномерно по туннелям.
  - **Per-packet**. Балансировка по пакетам. При передаче пакеты распределяются равномерно по туннелям.
  - **Broadcast**. Широковещательная передача. Пакеты передаются одновременно во все туннели для исключения потерь.

- **Точка назначения**.

- **Тип точки сбора**.

  Доступные значения:

  - **Сервисный интерфейс**. Отдельный сервисный интерфейс.
  - **Транспортный сервис**. Сервисный интерфейс, используемый в транспортном сервисе.

- **Тип транспортного сервиса** и **Транспортный сервис**. Параметры, позволяющие указать, в каком транспортном сервисе используется требуемый сервисный интерфейс. Вы можете указать значения для этих параметров только если в раскрывающемся списке **Тип точек сбора** вы выбрали **Транспортный сервис**.

- **Точки сбора**. 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.

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.

Чтобы выполнить отложенную задачу вручную:

1. В навигационной панели перейдите в раздел **Планировщик**.
2. Установите флажок рядом с одной или несколькими отложенными задачами, которые вы хотите выполнить вручную.
3. В раскрывающемся списке **Действия** выберите **Выполнить сейчас**.
4. В окне подтверждения нажмите на кнопку **Выполнить сейчас**.

Выбранные задачи будут выполнены незамедлительно.

Параметры контроллера SD-WAN

Параметры развернутого **контроллера SD-WAN** имеют значения по умолчанию. Эти параметры регулируют его работу, например параметр `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.

Каждый параметр контроллера SD-WAN имеет *метод изменения*, который определяет, может ли значение параметра быть изменено и в какой момент изменение вступает в силу. Параметры могут иметь следующие методы изменения:

- **Read-only**. Параметр напрямую влияет на работу контроллера SD-WAN и не может быть изменен.
- **Reload**. Параметр может быть изменен. При изменении значения параметра **оркестратор** отправляет новое значение в базу данных контроллера SD-WAN. Новое значение параметра вступает в силу после перезагрузки контроллера. Значение параметра, которое находится в базе данных, но еще не вступило в силу, называется *планируемым значением*. Вы можете удалить планируемое значение параметра 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**. Параметр может быть изменен. Новое значение параметра вступает в силу сразу после изменения.

Вы можете изменять параметры с методами изменения Reload и Runtime, сбрасывать их до значений по умолчанию, а также удалять планируемые значения параметров.

Если ваш контроллер SD-WAN развернут в виде кластера из нескольких узлов, вам нужно открыть страницу настройки кластера, чтобы изменить параметры контроллера. Вы не можете изменять параметры контроллера SD-WAN на странице настройки одного из его узлов.

Изменение и сброс параметров контроллера SD-WAN

Изменения, которые вы вносите в параметры контроллера SD-WAN с методом изменения Runtime, сразу вступают в силу. Если вы изменяете или сбрасываете параметр контроллера SD-WAN с методом изменения Reload, вам нужно перезагрузить контроллер, чтобы изменения вступили в силу.

Чтобы изменить или сбросить параметры контроллера SD-WAN до значений по умолчанию:

1. В разделе со списком параметров контроллера выберите вкладку **Изменяемые параметры**.
2. Если необходимо сбросить все параметры контроллера до значений по умолчанию:

a. Над списком параметров 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. Если необходимо сбросить отдельный параметр до значения по умолчанию:

a. Нажмите на кнопку **Управление** рядом с требуемым параметром контроллера и в раскрывающемся списке выберите **Сбросить параметр до значения по умолчанию**.

b. В окне подтверждения нажмите на кнопку **Сбросить**.

4. Если необходимо изменить значение параметра:

a. Нажмите на кнопку **Управление** рядом с параметром контроллера и в раскрывающемся списке выберите **Изменить**.

b. В открывшемся окне в поле **Планируемое значение** введите новое значение параметра.

c. Нажмите на кнопку **Сохранить**.

Если вы изменили параметр контроллера SD-WAN с методом изменения Runtime, новое значение отобразится в столбце **Текущее значение** списка параметров контроллера. Новое значение параметра с методом изменения Reload отобразится в столбце **Планируемое значение**.

Если вы хотите отменить запланированные изменения параметров контроллера, вам нужно удалить запланированные значения этих параметров. Это действие применимо только к параметрам с методом изменения Reload.

Чтобы удалить запланированные значения параметров контроллера:

1. В разделе со списком параметров контроллера выберите вкладку **Изменяемые параметры**.

2. Если необходимо удалить запланированные значения для всех параметров:

a. Над списком параметров контроллера нажмите на кнопку настройки и в раскрывающемся списке выберите **Удалить все запланированные значения**.

b. В окне подтверждения нажмите на кнопку **Удалить**.

3. Если необходимо удалить запланированное значение отдельного параметра:

a. Нажмите на кнопку **Управление** рядом с требуемым параметром и в раскрывающемся списке выберите **Удалить запланированное значение**.

b. В окне подтверждения нажмите на кнопку **Удалить**.

Запланированные значения параметров 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 параметров с методом изменения Reload вступили в силу. Если контроллер SD-WAN 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 **Flavours**. 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 параметров контроллера SD-WAN, на вкладке **Изменяемые параметры** планируемые значения параметров 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 решения отображаются все узлы контроллера SD-WAN – основной и второстепенные (если используются). Вы можете просматривать статистику работы каждого узла, а также список их параметров с указанными значениями.

Чтобы просмотреть информацию об узлах контроллера SD-WAN:

1. В дополнительном меню настройки решения перейдите в раздел **Узлы контроллера**.
2. Для просмотра статистики работы узла нажмите на кнопку **Управление** рядом с выбранным узлом и в раскрывающемся списке выберите **Статистика**.
3. Для просмотра параметров узла нажмите на кнопку **Управление** рядом с выбранным узлом 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 решения перейдите в раздел **Топология**.
2. Если требуется, в правом верхнем углу страницы установите следующие флажки:

   - **Загруженность каналов**. Флажок, позволяющий показать загруженность отображенных туннелей.

     Уровень загруженности туннеля соответствует следующим цветам:

     - Зеленый. Малая загруженность туннеля.

- Желтый. Средняя загруженность туннеля.
- Красный. Высокая загруженность туннеля.

- **Сегменты**. Флажок, позволяющий выбрать два устройства CPE в раскрывающемся списке **Выберите два коммутатора**, после чего отобразить все туннели, используемые в выбранном сегменте.
- **Внутриполосное управление**. Флажок, позволяющий 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**. Флажок, позволяющий отобразить имена устройств CPE, используемых в топологии.
- **IP-адрес**. Флажок, позволяющий отобразить IP-адреса устройств CPE, используемых в топологии.

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

Control plane

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

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.

Data plane

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

Physical Network Function (PNF)

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

PNF package

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

VNF package

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

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.

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.