kaspersky

Kaspersky SD-WAN

Руководство по планированию и внедрению

Версия программы:

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 12.12.2022

https://www.kaspersky.ru
https://help.kaspersky.com/ru
https://support.kaspersky.ru

О "Лаборатории Касперского": https://www.kaspersky.ru/about/company

kaspersky

Содержание

kaspersky

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com (https://community.kaspersky.com/)

kaspersky

Предоставление данных

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

kaspersky

Kaspersky SD-WAN

Решение Kaspersky SD-WAN (далее также решение) используется для построения программно-определяемых распределенных сетей (англ. Software Defined WAN, далее также сети SD-WAN) для маршрутизации трафика по каналам сети передачи данных с применением технологии SDN (Software Defined Networking). В сетях SD-WAN наиболее эффективные пути маршрутизации трафика определяются автоматически.

Технология SDN подразумевает разделение уровня управления сетью (англ. Control Plane) и уровня передачи данных (англ. Data Plane). Уровень управления контролирует передачу пакетов по сети через телекоммуникационное оборудование, установленное на площадке клиента (англ. Customer Premises Equipment, далее также устройства CPE). Передача пакетов через устройства CPE осуществляется на уровне передачи данных.

В сетях, построенных с применением технологии SDN, уровень управления переносится в централизованный контроллер SD-WAN. Этот контроллер взаимодействует с устройствами CPE, составляющими уровень передачи данных, а также с оркестратором, который управляет сетью SD-WAN и имеет веб-интерфейс. Вы также можете управлять сетью SD-WAN с помощью API.

Решение Kaspersky SD-WAN предназначено для операторов связи, а также компаний, имеющих крупную филиальную сеть, и используется для замены стандартных маршрутизаторов в распределенных сетях. Процесс развертывания не зависит от транспортных технологий, используемых в вашей сети. С помощью этого решения вы можете выполнять следующие задачи:

- интеллектуальное управление трафиком;
- автоматическая настройка устройств CPE;
- централизованное управление инфраструктурой сети;
- мониторинг топологии сети и автоматическое реагирование на ее изменение;
- автоматическое реагирование на изменение требований приложений к качеству обслуживания (англ. Quality of Service, далее также QoS);
- управление решением через веб-интерфейс оркестратора.

Чтобы развернуть решение Kaspersky SD-WAN, вам нужно создать виртуальные каналы на основе существующих транспортных сервисов. Для создания виртуальных каналов вы можете использовать следующие транспортные сервисы:

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

Вы можете создать несколько виртуальных каналов и использовать их для передачи трафика с учетом требований приложений к пропускной способности и качеству обслуживания.

Решение Kaspersky SD-WAN обладает следующими характеристиками:

- Независимость от используемых физических сетей (англ. Underlay Network).

  Решение может работать на основе проводных и беспроводных сетей любого типа.

- Постоянный мониторинг виртуальных каналов.

Решение автоматически переключается на резервный маршрут в случае обнаружения сбоя в работе виртуального канала.

- Возможность создать несколько виртуальных каналов.

  Решение позволяет создать несколько виртуальных каналов для обеспечения высокой доступности сети.

- Централизованное управление.

  Решение имеет веб-интерфейс оркестратора для управления виртуальными каналами и их контроля, а также для автоматической настройки устройств CPE.

См. также

Настройка устройств CPE 28

Управление трафиком 45

kaspersky

Архитектура решения

Решение Kaspersky SD-WAN содержит следующие компоненты:

- **Оркестратор SD-WAN**.

  Компонент управления решением и устройствами CPE, который имеет графический веб-интерфейс. Оркестратор может управлять несколькими сервисами SD-WAN. Например, вы можете создать отдельный сервис SD-WAN для одного из филиалов вашей компании. Каждый сервис SD-WAN имеет собственный кластер контроллеров SD-WAN и шлюзы SD-WAN.

- **Контроллер SD-WAN**.

  Централизованный контроллер, который управляет наложенной сетью (англ. Overlay Network). Он обеспечивает построение топологии сети и создание транспортных сервисов внутри наложенных туннелей. Решение Kaspersky SD-WAN поддерживает транспортные сервисы L2 Point-to-Point (P2P), Point-to-Multipoint (P2M), Multipoint-to-Multipoint (M2M) и L3 VPN. Контроллер SD-WAN управляет устройствами CPE и шлюзами SD-WAN по протоколу OpenFlow.

- **Шлюзы SD-WAN**.

  Обязательные элементы сети, которые объединяют устройства CPE в единую сеть. Наложенные туннели терминируются на шлюзах SD-WAN, после чего трафик передается дальше в соответствии с топологией сети. Для обеспечения отказоустойчивости, шлюзы SD-WAN устанавливаются парами.

- **Устройства CPE**.

  Телекоммуникационное оборудование, которое подключается к шлюзам SD-WAN с помощью наложенных туннелей и образует SDN-фабрику в виде наложенной сети.

- **Менеджер виртуальных сетевых функций (англ. Virtual Network Function Manager, далее также VNFM).**

  Менеджер, который обеспечивает настройку виртуальных сетевых функций (англ. Virtual Network Functions, далее также VNF) и устройств CPE. *Виртуальные сетевые функции* – это сетевые функции, которые реализуются в виде программ на обычных компьютерных платформах COTS (Commercial Off The Shelf).

Все компоненты решения размещаются в Центре Обработки Данных (далее также ЦОД), за исключением устройств CPE, которые вам нужно разместить на требуемых площадках. Контролер и шлюзы SD-WAN разворачиваются в сети как VNF или отдельные виртуальные машины. Отдельные виртуальные машины, выполняющие функции контроллеров или шлюзов SD-WAN добавляются в каталог веб-интерфейса оркестратора как физические сетевые функции (англ. Physical Network Functions, далее также PNF). *Физические сетевые функции* – это сетевые функции, которые реализуются с помощью специального оборудования.

Решение подразумевает создание отдельного сервиса SD-WAN для каждого тенанта. *Тенант* – это логический пул ресурсов сети, предоставленный филиалу вашей компании или клиенту. Тенанты используются для обеспечения независимости сетей SD-WAN разных организаций друг от друга.

Если требуется построить сеть SD-WAN для нескольких клиентов с использованием ограниченного количества устройств CPE, то вы можете использовать решение Kaspersky SD-WAN для создания одного транспортного тенанта, внутри которого создаются тенанты отдельных клиентов. В этом случае тенанты делят между собой контроллер и шлюзы SD-WAN, но имеют отдельные устройства CPE, транспортные сервисы и веб-интерфейсы оркестратора.

При развертывании сервиса SD-WAN с использованием VNF в архитектуру решения входят следующие дополнительные компоненты:

- **Контроллер домена (англ. Domain Controller).**

  Контроллер, который обеспечивает создание виртуальных каналов (англ. Virtual Links) между VNF в ЦОД.

- **VIM.**

  Менеджер виртуальной инфраструктуры, который обеспечивает управление вычислительными и сетевыми ресурсами, а также ресурсами хранения. Все эти ресурсы необходимы для работы VNF.

Решение Kaspersky SD-WAN имеет распределенную микросервисную архитектуру, которая построена с помощью Docker-контейнеров (см. рисунок ниже).

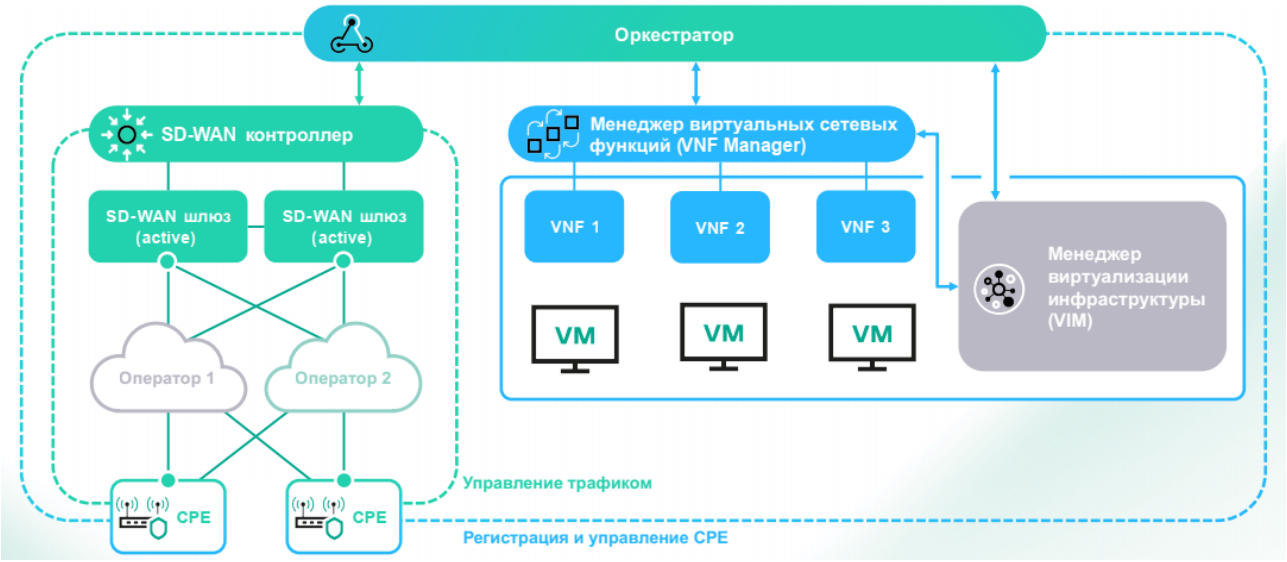

Рисунок 1. Архитектура решения Kaspersky SD-WAN

Перед развертыванием сервиса SD-WAN вам нужно создать тенант в веб-интерфейсе оркестратора. Внутри созданного тенанта требуется запустить сетевой сервис SD-WAN Network Service (далее также SD-WAN NS). Этот сетевой сервис состоит из VNF или PNF. Сервисная цепочка может состоять из устройств CPE, SD-WAN NS, а также из VNF, развернутых в ЦОД.

Контроллер SD-WAN может состоять из одного узла или кластера из трех узлов. Узлы кластера контроллера SD-WAN и шлюзы SD-WAN являются отдельными виртуальными машинами и могут запускаться на разных аппаратных серверах для обеспечения отказоустойчивости.

См. также

kaspersky

Масштабирование решения. Аппаратные и программные требования

Сеть SD-WAN, построенная с использованием решения Kaspersky SD-WAN, может состоять из одного или нескольких доменов SD-WAN. *Домен SD-WAN* – это основной компонент сети SD-WAN, имеющий две плоскости – data и control.

Плоскость data (англ. data plane) является сетевой абстракцией, которая объединяет подсистемы компонентов решения, осуществляющие коммутацию и маршрутизацию трафика.

Плоскость control (англ. control plane) является сетевой абстракцией, которая объединяет подсистемы компонентов решения, осуществляющие формирование правил коммутации и маршрутизации трафика.

Каждый домен содержит отдельный контроллер SD-WAN (или кластер контроллеров), одну или несколько пар шлюзов SD-WAN, а также площадки, на которых установлены устройства CPE (см. рисунок ниже). Вам нужно использовать VNFM (см. раздел "Архитектура решения" на стр. 10), чтобы развернуть требуемый домен в виде отдельной VNF. Для расширения сети SD-WAN вы можете развернуть дополнительные домены, таким образом создавая *мультидомен SD-WAN*.

Мультидомен SD-WAN может иметь несколько data- и control-плоскостей, а также дополнительную плоскость management. Эта плоскость является сетевой абстракцией, которая объединяет подсистемы компонентов решения, осуществляющие настройку всех компонентов и мониторинг их работы.
В management-плоскости происходит взаимодействие между пользователем и решением Kaspersky SD-

WAN. Если ваша сеть SD-WAN построена с использованием одного домена SD-WAN, то этот домен имеет все три плоскости – data, control и management.

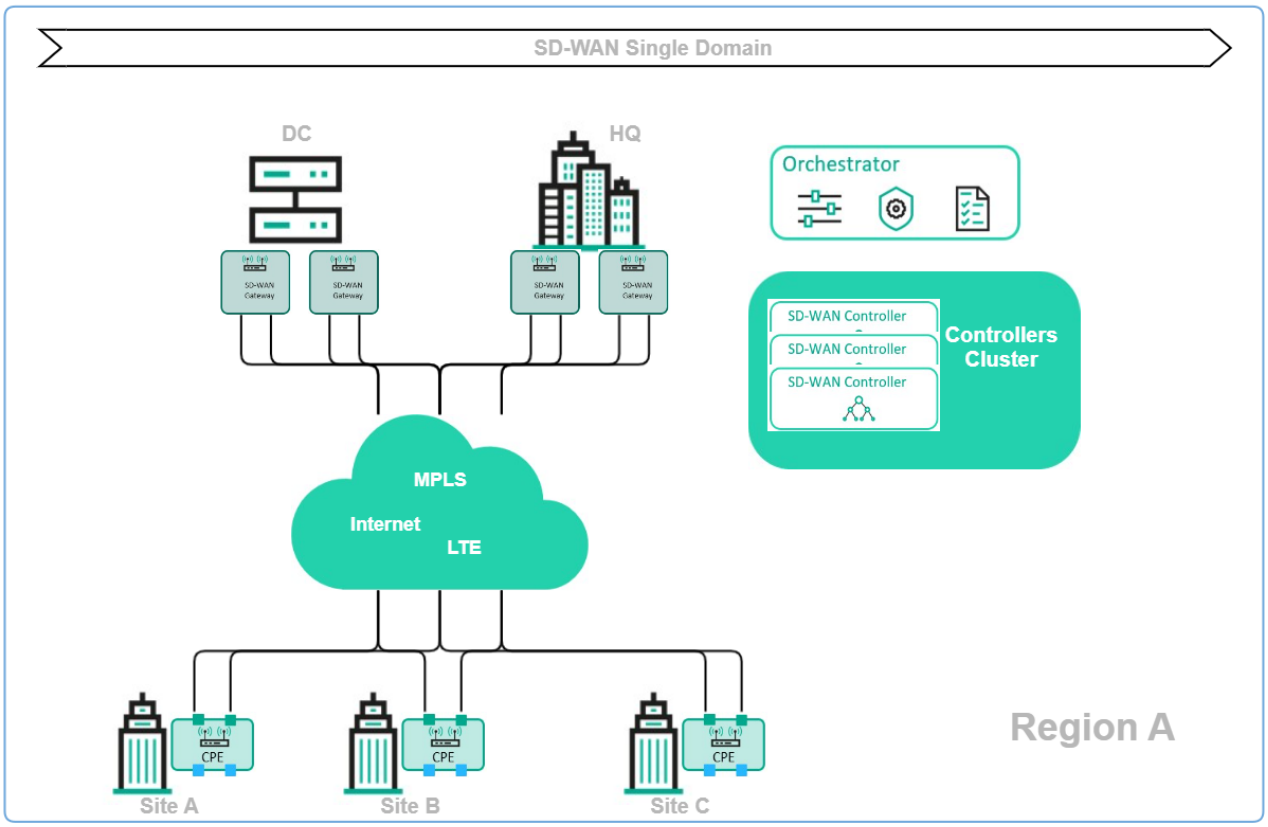

Рисунок 2. Компоненты домена SD-WAN

Площадки, на которых установлены устройства CPE, могут быть объединены в один домен по различным причинам, актуальным для вашей организации, например:

- площадки расположены близко друг к другу;
- площадки имеют схожие сетевые топологии;
- площадки имеют высокую долю локального трафика;
- площадки относятся к зоне ответственности одного сетевого администратора;
- пользователи площадок предпочитают использовать централизованные или облачные сервисы.

Для установления подключения между устройствами CPE, которые относятся к разным доменам, используются шлюзы SD-WAN, развернутые в рамках каждого домена (см. рисунок ниже). Использование нескольких доменов SD-WAN и привязка устройств CPE к этим доменам в соответствии с запросами

пользователей, обеспечивает наилучшее качество сервисов, предоставляемых на основе решения Kaspersky SD-WAN.

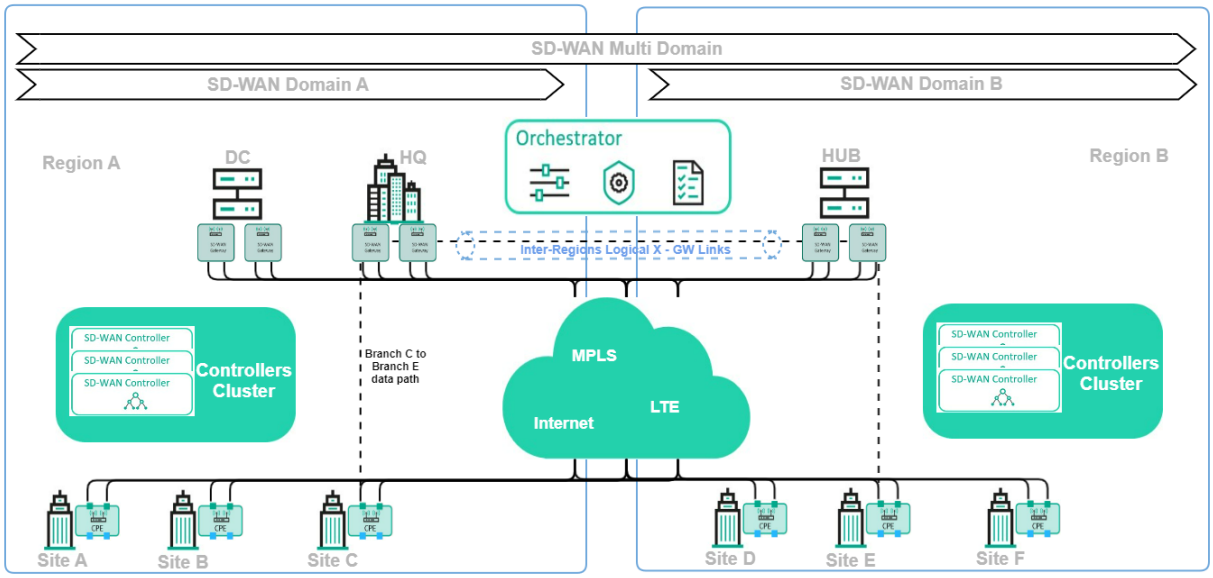

Рисунок 3. Компоненты мультидомена SD-WAN

Аппаратные и программные требования

Требования к аппаратным ресурсам зависят от количества управляемых устройств CPE, которые используются в вашей схеме развертывания решения Kaspersky SD-WAN (см. таблицы ниже).

Таблица 1. Аппаратные требования к серверам или виртуальным машинам для развертывания оркестратора SD-WAN

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

Таблица 2. 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
Менеджер виртуальных сетевых функций					
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 установке контейнеров для развертывания контроллера SD-WAN вы можете использовать переподписку с максимальным коэффициентом 3.

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.
- RedHat версии 7.1 и выше.
- SUSE версии 12.4 и выше.

Протестированные устройства CPE

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

Таблица 3. 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 (см. таблицу ниже). На тестируемых устройствах CPE не использовалась технология DPI (Deep Packet Inspection), а также было выключено шифрование трафика (на стр. 49).

Таблица 4. 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

Модель	Размер пакетов, байт	Пропускная способность (Мбит/сек)
Kraftway Рубеж-Т	IMIX (417)	2875
	Large (1300)	5750

kaspersky

Развертывание сервиса SD-WAN

В этом разделе содержится информация о том, как развернуть сервис SD-WAN. Вы можете развернуть контроллер и шлюзы SD-WAN в виде VNF и PNF. Для развертывания контроллера и шлюзов SD-WAN в виде PNF не требуется VIM.

В этом разделе

Развертывание сервиса SD-WAN в виде VNF

Для развертывания контроллера и шлюзов SD-WAN в сети в виде VNF требуется разместить каждый из следующих компонентов VNF на отдельной виртуальной машине:

- SD-WAN Controller.
- SD-WAN Gateway1.
- SD-WAN Gateway2.

Размещение компонентов VNF на виртуальных машинах и последующее управление VNF осуществляется с помощью пакета VNF (англ. VNF Package). *Пакет VNF* – это архив в формате TAR или ZIP, который содержит следующие данные:

- Образы виртуальных машин для контроллера и шлюзов SD-WAN.

  Файлы образов имеют формат QCOW2.

- VNF-дескриптор.

  Файл с именем vnfd.xml, который описывает параметры VNF и имеет формат XML.

- Папка со скриптами.

  Скрипты используются для развертывания и управления VNF. Для управления конфигурацией виртуальных машин используются файлы-сценарии Ansible playbook.

Пакет VNF может содержать один контроллер SD-WAN или кластер контролеров, состоящий из трех узлов.

Для добавления VNF в каталог веб-интерфейса оркестратора вам нужно перейти в раздел **Каталог** (). Вы можете использовать VNF, добавленные в каталог веб-интерфейса оркестратора, для создания шаблона сервиса SD-WAN. В ходе создания шаблона вы можете смотреть и изменять основные параметры VNF и виртуальных машин, например IP-адреса и порты для подключения устройств CPE. Созданный шаблон можно использовать для развертывания сервиса SD-WAN.

Развертывание сервиса SD-WAN в виде PNF

Для развертывания контроллера и шлюзов SD-WAN в виде PNF требуется воспользоваться *пакетом PNF* (англ. PNF Package). В отличие от пакета VNF, который используется для развертывания контроллера и шлюзов SD-WAN в виде VNF, пакет PNF не содержит папку images и файл дескриптора называется pnfd.xml. В остальном содержание пакетов PNF и VNF идентично.

Перед добавлением PNF в каталог веб-интерфейса оркестратора требуется развернуть контроллер (или кластер контроллеров) и два шлюза SD-WAN. Оркестратор не создает виртуальные каналы для PNF, поэтому вам нужно заранее настроить сетевые интерфейсы и установить IP-связность между оркестратором и PNF, а также между компонентами PNF. Для добавления PNF в каталог веб-интерфейса оркестратора вам нужно перейти в раздел **Каталог** ().

Чтобы использовать PNF в сервисных цепочках, до развертывания сервиса SD-WAN нужно добавить требуемые точки подключения (англ. connection points). В качестве точек подключения требуется указать сервисные интерфейсы, например коммутатор, порт или VLAIN ID. Для одной точки подключения можно указать несколько сервисных интерфейсов. Вы можете не указывать сервисные интерфейсы. В этом случае PNF невозможно использовать при создании сервисной цепочки в веб-интерфейсе оркестратора.

См. также

Развертывание сервиса SD-WAN в виде VNF 18

О шаблоне экземпляра SD-WAN

Шаблон экземпляра SD-WAN (англ. SD-WAN Instance template) содержит параметры наложенной SDN-сети. Вам нужно применить его к контроллеру SD-WAN после развертывания сервиса SD-WAN. Для добавления шаблона экземпляра SD-WAN вам нужно перейти в раздел **SD-WAN** () веб-интерфейса оркестратора, после чего перейти в подраздел **SD-WAN шаблоны экземпляров** (). Чтобы настроить шаблон экземпляра SD-WAN, вы можете использовать вкладки, которые отображаются в верхней части шаблона (см. таблицу ниже).

Таблица 5. Описание шаблона экземпляра SD-WAN

Вкладка	Описание
Информация	На этой вкладке отображается название шаблона экземпляра SD-WAN. Если требуется, вы можете изменить название шаблона.
Сопоставление портов GW	На этой вкладке вы можете добавить OpenFlow-порты шлюзов SD-WAN GW1 и SD-WAN GW2. Решение Kaspersky SD-WAN использует эти порты для создания транспортных сервисов.
Настройки CoS	На этой вкладке вы можете создать классы обслуживания, чтобы использовать их в сети SD-WAN. Один из классов обслуживания можно использовать для трафика реального времени, для которого требуется обеспечить минимальную потерю пакетов. Вы не можете создать больше восьми классов обслуживания. При создании класса обслуживания вам потребуется выбрать внутреннюю метку (внутренний тег) и назначить очередь для обработки трафика этого класса обслуживания. Мы рекомендуем не менять значения по умолчанию в полях **KOver** и **Максимальная зарезервированная пропускная способность (%)**.
Классификаторы	На этой вкладке вы можете создать классификаторы трафика. *Классификатор трафика* определяет, доверять меткам качества обслуживания, выставленным во входящих пакетах, или нет. Чтобы классификатор доверял меткам качества обслуживания, при его создании требуется выбрать тип классификатора **Trust** и установить соответствия между значениями, которые содержатся в полях **DSCP** или **VLAN PCP** заголовков входящих пакетов, и ранее созданными классами обслуживания.
QoS правила	На этой вкладке вы можете создать правила качества обслуживания, чтобы ограничить полосу пропускания для трафика, входящего в транспортный сервис. Вы также можете указать доступную полосу пропускания для каждого класса трафика в процентах от общей полосы пропускания.

Вкладка	Описание
Сервисы	На этой вкладке вы можете создать шаблоны транспортных сервисов. Решение Kaspersky SD-WAN использует транспортные сервисы для передачи данных между устройствами CPE и шлюзами SD-WAN. Транспортные сервисы P2M и M2M должны содержать как минимум два сервисных интерфейса. Чтобы создать шаблон транспортного сервиса P2M, вам нужно выбрать роль Root или Leaf для каждого сервисного интерфейса. Пакеты, приходящие на сервисный интерфейс с ролью Root, могут быть направлены в сервисные интерфейсы с любой ролью, в то время как пакеты, приходящие на сервисный интерфейс с ролью Leaf, могут быть направлены только в сервисный интерфейс с ролью Root. При создании шаблона транспортного сервиса вам нужно выбрать правило качества обслуживания. Вы можете создавать правила качества обслуживания на вкладке **QoS правила**. При создании сервисного интерфейса для транспортного сервиса, необходимо указать следующую информацию: • устройство и порт, используемые для создания точки подключения; • тип инкапсуляции, например Access, VLAN или QinQ; • значение метки VLAN ID для инкапсуляции VLAN; • значение внешней и внутренней метки VLAN ID для инкапсуляции QinQ. Вам нужно указать только сервисные интерфейсы на шлюзах SD-WAN. Когда вы подключаете устройство CPE, принадлежащие ему сервисные интерфейсы автоматически добавляются к транспортным сервисам. При создании шаблона CPE требуется указать список транспортных сервисов и параметры сервисных интерфейсов. По умолчанию шаблон экземпляра SD-WAN содержит транспортный сервис P2M SD-WAN managementTunnel. Этот транспортный сервис необходим для управления сетью SD-WAN.
Арендаторы	На этой вкладке вы можете добавить или удалить тенантов, которые используют шаблон экземпляра SD-WAN. Если вы не хотите, чтобы тенант использовал шаблон по умолчанию, то вам нужно привязать требуемый шаблон к тенанту до развертывания сервиса SD-WAN.
High Availability	На этой вкладке вы можете выбрать количество узлов контроллера SD-WAN.

Вы можете создать несколько шаблонов экземпляра SD-WAN. При развертывании решения автоматически создается шаблон экземпляра SD-WAN, который используется по умолчанию. Этот шаблон невозможно удалить, но вы можете использовать другой шаблон в качестве шаблона по умолчанию. Если при развертывании сервиса SD-WAN к тенанту не привязывается шаблон экземпляра SD-WAN, то к этому тенанту привязывается шаблон по умолчанию.

kaspersky

См. также

Шаблон экземпляра SD-WAN по умолчанию

Шаблон экземпляра SD-WAN по умолчанию создается после развертывания решения. Он отображается в подразделе **SD-WAN шаблоны экземпляров** (). На вкладках этого шаблона отображаются параметры по умолчанию.

На вкладке **Сопоставление портов GW** добавлены следующие порты**:**

- На вкладке **GW1** добавлен порт 1.

  Этот порт первого (основного) шлюза SD-WAN подключается к сети управления.
- На вкладке **GW1** добавлен порт 3.

  Этот порт первого (основного) шлюза SD-WAN подключается к локальной сети ЦОД.
- На вкладке **GW2** добавлен порт 1.

  Этот порт второго (резервного) шлюза SD-WAN подключается к сети управления.
- На вкладке **GW2** добавлен порт 3.

  Этот порт второго (резервного) шлюза SD-WAN подключается к локальной сети ЦОД.

На вкладках **Настройки CoS**, **Классификаторы** и **QoS правила** указаны следующие параметры:

- весь трафик попадает в класс **Best Effort**;
- полоса пропускания трафика не ограничивается.

На вкладке **Сервисы** созданы два транспортных сервиса (см. таблицу ниже).

Таблица 6. Описание транспортных сервисов по умолчанию

Параметр	Транспортный сервис 1	Транспортный сервис 2
Название транспортного сервиса	`SD-WAN managementTunnel`.	`SD-WAN P2M Data`.
Топология транспортного сервиса	**P2M**.	**P2M**.
Время, по прошествии которого адрес удаляется из таблицы MAC-адресов	`3600`	`3600`.
Максимальный размер таблицы MAC-адресов	`2000`.	`2000`.
Режим работы транспортного сервиса	**Classic**.	**Classic**.
Интерфейсы транспортного сервиса	Основной интерфейс имеет следующие параметры: • Название: `GW1`. • Порт: `1`. • Тип инкапсуляции: **Access**. • Правило качества обслуживания: **QoS Unlimited-QoS**. • Роль: **ROOT**. Резервный интерфейс имеет следующие параметры: • Название: `GW2`. • Порт: `1`. • Тип инкапсуляции: **Access**.	Основной интерфейс имеет следующие параметры: • Название: `GW1`. • Порт: `3`. • Тип инкапсуляции: **Access**. • Правило качества обслуживания: **QoS Unlimited-QoS**. • Роль: **ROOT**. Резервный интерфейс имеет следующие параметры: • Название: `GW2`. • Порт: `3`. • Тип инкапсуляции: **Access**.

См. также

О шаблоне экземпляра SD-WAN.....19

О тенантах

Вы можете создавать тенанты, чтобы предоставлять сетевые ресурсы требуемым площадкам.

Для создания тенантов вам нужно перейти в раздел **Арендаторы** ( ) веб-интерфейса оркестратора. Каждый тенант имеет следующие элементы:

- Группа VIM.

  Используется для создания виртуальных машин, входящих в VNF.

- Сервисные интерфейсы (англ. User Network Interface, UNI).

Используются для указания точек входа и выхода трафика сетевого сервиса. Для каждого сервисного интерфейса требуется указать информацию о коммутаторе OpenFlow, порте и типе инкапсуляции. Вы можете не указывать сервисные интерфейсы при создании тенанта.

- Пользователи и группы пользователей.

  Используются для указания пользователей, которые имеют доступ к тенанту.

- Каталог.

  Используются для построения сетевых сервисов с помощью шаблонов сетевых сервисов и VNF.

Вам нужно создать учетную запись для каждого тенанта и назначить роль администратора тенанта требуемым пользователям. *Администратор тенанта* может выполнять следующие задачи в рамках предоставленных сетевых ресурсов:

- просмотр топологии сети и управление компонентами сети;
- создание, удаление и изменение сетевых сервисов;
- просмотр загрузки компонентов сети;
- управление VNF;
- мониторинг состояния сети.

После создания тенанта вы можете подключиться к нему в качестве администратора для изменения параметров и устранения неполадок. Вы также можете предоставить тенантам доступ к созданным шаблонам сервисов SD-WAN.

См. также

О шаблоне экземпляра SD-WAN.....19

Сценарий: развертывание сервиса SD-WAN для тенанта 26

Настройка параметров контроллера SD-WAN

После развертывания контроллера SD-WAN вы можете изменить его параметры. Значения параметров регулируют работу контроллера SD-WAN, например параметр `controller.listen.port` определяет TCP-порт для входящих соединений, к которому подключаются устройства CPE.

Для настройки параметров контроллера SD-WAN вам нужно перейди в раздел **Инфраструктура** () веб-интерфейса оркестратора, после чего открыть страницу настройки параметров требуемого контроллера SD-WAN.

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 веб-интерфейс оркестратора отправляет новое значение в базу данных контроллера SD-WAN. Новое значение параметра вступает в силу после перезагрузки контроллера SD-WAN. Значение параметра, которое находится в базе данных оркестратора, но еще не вступило в силу, называется *планируемым значением*. Вы можете удалить планируемое значение параметра до перезагрузки контроллера SD-WAN, чтобы сохранить текущее значение.

- Runtime.

  Параметр может быть изменен. Новое значение параметра вступает в силу сразу после изменения.

Для настройки параметров с методами изменения Reload и Runtime используется вкладка **Изменяемые свойства**. Вы можете посмотреть информацию о каждом параметре с помощью столбцов, которые отображаются в верхней части вкладки (см. таблицу ниже).

Таблица 7. Информация о параметрах контроллера SD-WAN

Параметр	Описание
Метод Изменения	Метод изменения параметра. Параметры, которые отображаются на вкладке **Изменяемые свойства** могут иметь методы изменения Reload и Runtime. Для просмотра параметров с методом изменения Read-only вам нужно выбрать вкладку **Все свойства**.
Свойства	Название параметра.
Текущее значение	Значение параметра.
Планируемое значение	Планируемое значение параметра. Только параметры с методом изменения Reload могут иметь планируемые значения. После того, как вы перезагружаете контроллер SD-WAN, значения из столбца **Планируемое значение** переносятся в столбец **Текущее значение**.

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 трех узлов, то вам нужно открыть страницу настройки кластера, чтобы изменить параметры контроллера. Вы не можете изменить параметры контроллера SD-WAN с помощью страницы настройки одного из его узлов.

Сценарий: развертывание сервиса SD-WAN для тенанта

В этом разделе представлен краткий сценарий развертывания сервиса SD-WAN для тенанта. Этот сценарий предназначен для администратора тенанта. Прежде чем администратор тенанта сможет развернуть сервис SD-WAN, вам нужно привязать к этому тенанту требуемые сервисные интерфейсы и шаблон сервиса SD-WAN. После завершения этого сценария для тенанта будет развернут сервис SD-WAN.

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

a. **Выбор шаблона сервиса SD-WAN в каталоге веб-интерфейса оркестратора**

   Администратор тенанта может выбрать один из шаблонов сервиса SD-WAN, которые вы создали и привязали к тенанту. Для выбора шаблона сервиса SD-WAN администратору тенанта нужно перейти в раздел **Каталог** ( ) веб-интерфейса оркестратора.

b. **Настройка сервиса SD-WAN**

Администратор тенанта может изменить параметры сервиса SD-WAN с помощью графического конструктора. В графическом конструкторе администратору нужно заменить абстрактные сервисные интерфейсы на реальные, после чего ввести имя сервиса SD-WAN и сохранить его.

c. **Развертывание сервиса SD-WAN**

Администратор тенанта может развернуть сервис SD-WAN и приступить к настройке устройств CPE.

Для настройки устройств CPE администратору тенанта нужно перейти в раздел **SD-WAN** () веб-интерфейса оркестратора, после чего автоматически откроется раздел **CPE инвентарь** ().

См. также

kaspersky

Настройка устройств CPE

В этом разделе содержится информация о том, какие устройства CPE поддерживаются решением Kaspersky SD-WAN. В разделе также описана настройка устройств CPE.

Решение поддерживает следующие основные требования к устройствам CPE, которые могут быть установлены на клиентских площадках или в филиалах вашего офиса:

- стандартная архитектура процессора x86 или Arm/MIPS;
- отсутствие зависимости от определенных производителей;
- минимальные характеристики аппаратных ресурсов, таких как процессор и операционная память.

При построении сети SD-WAN с помощью Kaspersky SD-WAN вы можете использовать устройства CPE двух типов:

- Устройства CPE, выполняющие исключительно транспортную функцию.

  Этот тип устройств CPE обеспечивает обмен трафиком между устройствами CPE, а также его доставку в ЦОД, который может предоставлять различные сетевые функции, например работу протоколов маршрутизации. Для предоставления сетевых функций из ЦОД или облака вам нужно интегрировать решение Kaspersky SD-WAN с решением vCPE (Virtual CPE). Эта интеграция делает возможной маршрутизацию трафика от устройства CPE в сервисную цепочку, существующую в ЦОД или облаке. Сервисная цепочка может включать в себя VNF, например виртуальную маршрутизацию, систему предотвращения вторжений или антивирус. После предоставления VNF трафик передается к месту назначения.

- Universal CPE (далее также uCPE).

  Этот тип устройств CPE дополнительно поддерживает запуск VNF. Устройство CPE должно иметь достаточно аппаратных ресурсов для того, чтобы не задействовать ЦОД или облако для предоставления VNF. Локальное размещение VNF улучшает время отклика, оптимизирует транспортные потоки и сохраняет возможность управлять uCPE с помощью веб-интерфейса оркестратора.

В этом разделе

kaspersky

Автоматическая настройка устройств CPE

Каждое устройство CPE имеет уникальный *идентификатор DPID* (Datapath Identifier). Это 64-битное число, которое генерируется на основании уникальной характеристики устройства CPE, например MAC-адреса порта WAN0 или серийного номера. Перед отправкой устройства CPE на требуемую площадку вам нужно добавить его в инвентаризационную базу веб-интерфейса оркестратора с указанием идентификатора DPID, шаблона CPE и тенанта, к которому устройство CPE будет привязано. Для добавления устройства CPE в инвентаризационную базу вам нужно перейти в раздел **SD-WAN** () веб-интерфейса оркестратора.

Этот раздел автоматически отображает подраздел **CPE инвентарь** ().

Подключение устройств CPE к контроллеру SD-WAN и их автоматическая настройка (англ. zero touch provisioning) осуществляется в следующей последовательности:

1. Устройство CPE получает IP-адреса WAN-портов и серверов DNS, а также маршруты по умолчанию от оператора связи по протоколу DHCP.
2. Устройство CPE использует полное имя домена (англ. Fully Qualified Domain Name, FQDN) оркестратора чтобы связаться с ним, сообщает свой идентификатор DPID и получает внешние IP-адреса контроллера и шлюзов SD-WAN.
3. Устройство CPE устанавливает соединение с контроллером SD-WAN по протоколу TLS через IP-сеть, используя сеть оператора или интернет.
4. Контроллер SD-WAN отправляет команды на устройство CPE для создания наложенных туннелей от каждого WAN-порта к шлюзам SD-WAN в составе сервиса SD-WAN для выбранного тенанта.
5. Контроллер SD-WAN программирует устройство CPE и шлюзы SD-WAN для создания транспортных сервисов в соответствии с требуемой топологией.

Чтобы автоматически настроить устройства CPE через интернет, требуется настроить внешние (англ. public) IP-адреса оркестратора, контроллера и шлюзов SD-WAN. Если у вас нет возможности настроить отдельные внешние IP-адреса, то вы можете настроить статический механизм Network Address Translation (NAT) для следующих портов:

- Порт tcp 443, 81 для оркестратора.
- Порт tcp 6653 для контроллера SD-WAN.
- Порты udp 4800–4819 для шлюзов SD-WAN.

  Номера и количество upd-портов зависят от количества WAN-портов на устройстве CPE.

Если устройство CPE, отсутствующее в инвентаризационной базе веб-интерфейса оркестратора, попытается зарегистрироваться в оркестраторе, оно будет отображаться в инвентаризационной базе веб-интерфейса оркестратора со статусом *Неизвестно*. Вы можете удалить это устройство или зарегистрировать его, указав тенанта, к которому относится устройство CPE.

О шлюзах SD-WAN

Сервис SD-WAN включает в себя два шлюза – основной и резервный. Каждый из этих шлюзов SD-WAN нужно развернуть на отдельной виртуальной машине и соединить их каналом Ethernet с пропуском заголовков VLAN согласно стандартам IEEE 802.1Q и 802.1ad. Шлюзы SD-WAN подключаются к интернету.

Все шлюзы SD-WAN имеют одинаковую логическую схему (см. рисунок ниже).

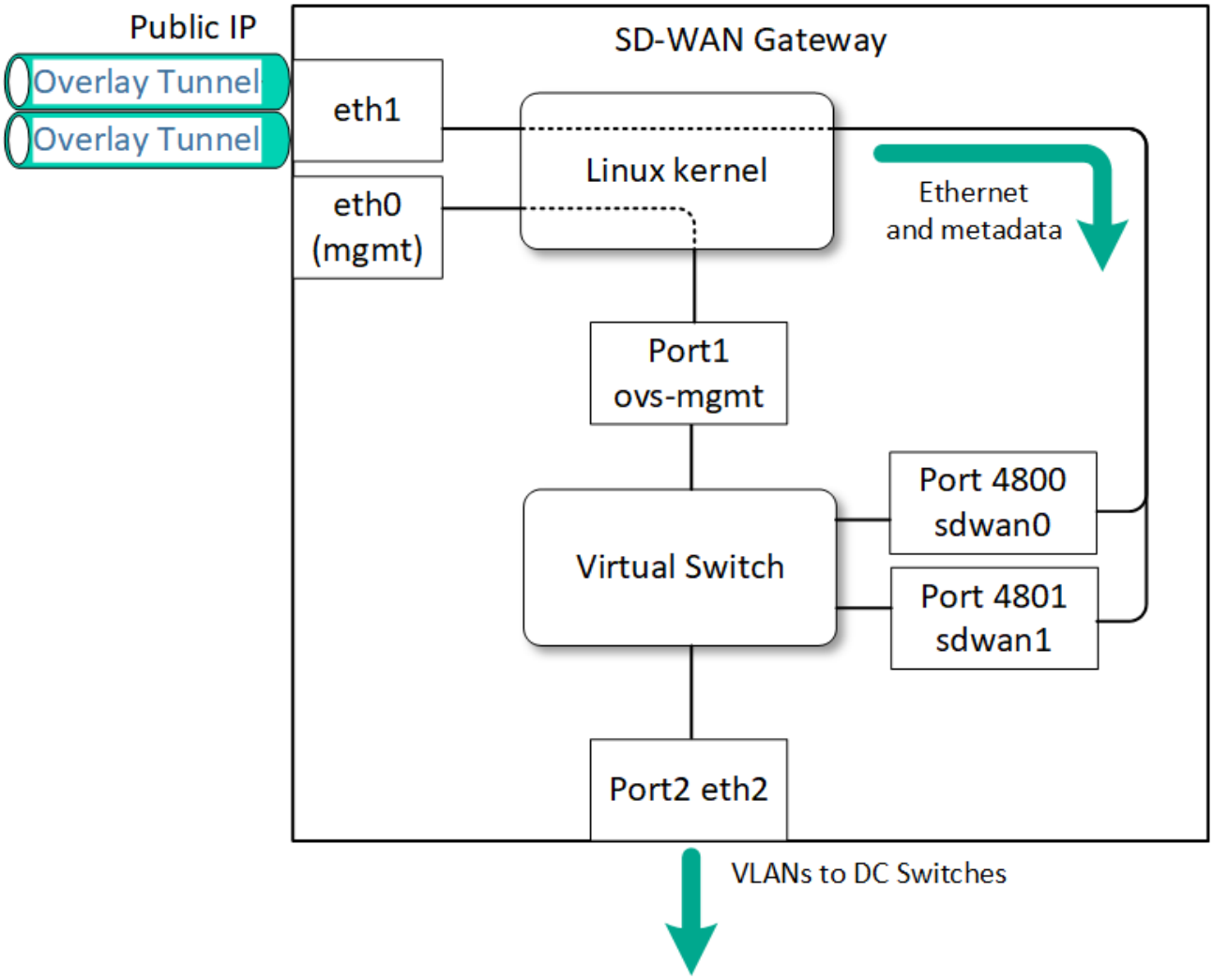

Рисунок 4. Логическая схема шлюзов SD-WAN

Вам нужно назначить выделенный публичный IP-адрес каждому шлюзу SD-WAN или использовать для них один IP-адрес, но разные UDP-порты. Каждый шлюз SD-WAN содержит следующие Ethernet-порты:

- eth0.

  Этот порт используется для управления шлюзом.

- eth1.

  Этот порт используется для терминации наложенных туннелей от устройств CPE.

- eth2.

  Этот порт используется для подключения шлюза SD-WAN к локальной сети ЦОД, создания виртуальных каналов с VNF и выхода в интернет.

В состав шлюза SD-WAN входит программный коммутатор OpenFlow, в который напрямую включаются порты eth2 и eth3. В него также включаются порты sdwan0 и sdwan1 типа VXLAN, каждый из которых имеет следующие параметры:

- в качестве IP-адреса источника указывается IP-адрес порта eth1;
- на первом шлюзе:
  - номер порта sdwan0 – 4800;
  - номер порта sdwan1 – 4801;
- на втором шлюзе:
  - номер порта sdwan0 – 4810;
  - номер порта sdwan1 – 4811;

Если устройства CPE, которые вы планируете подключить к шлюзам SD-WAN, имеют больше двух WAN-портов, то вам нужно увеличить количество sdwan-портов на шлюзах. Новым портам sdwan присваиваются следующие по порядку номера.

Программный коммутатор OpenFlow управляется контроллером SD-WAN и имеет следующие порты OpenFlow:

- Port 1 (Port mgmt).

  Этот порт включается в сервис управления SD-WAN ManagementTunnel.
- Port 2 (eth2).

  Этот порт используется для создания транспортных сервисов, которые передают трафик от устройств CPE.
- Port 4800–4801 для первого шлюза и 4810–4811 для второго шлюза.

  Эти порты являются транзитными.

Об устройствах CPE

Каждое устройство CPE имеет следующие внешние порты:

- Один или несколько LAN-портов.

  Вы можете объединить несколько LAN-портов в коммутатор с помощью Linux-мостов.
- Один или несколько WAN-портов.

  Эти порты могут иметь проводную или беспроводную среду передачи. Каждый порт получает параметры IPv4 по протоколу DHCP.

Все устройства CPE имеют одинаковую логическую схему (см. рисунок ниже).

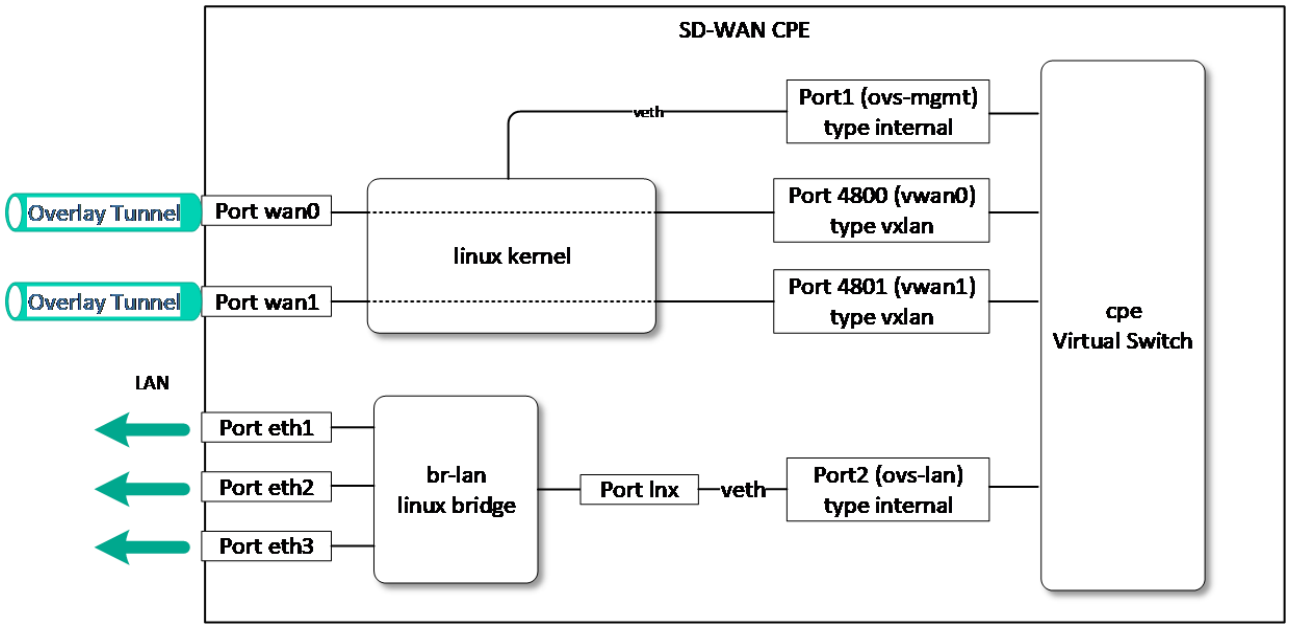

Рисунок 5. Логическая схема устройства CPE

Каждое устройство CPE имеет внутренний порт mgmt, который используется для удаленной настройки этого устройства после подключения к оркестратору и контроллеру SD-WAN.

Устройства CPE также имеют программные коммутаторы OpenFlow (англ. CPE virtual switch), которые управляются контроллером SD-WAN. Каждый программный коммутатор OpenFlow имеет следующие порты:

- Port 1 (ovs-mgmt).

  Этот порт используется для организации внутреннего управления сетью и настройки устройства CPE через сервис управления SD-WAN managementTunnel после подключения устройства CPE к контроллеру SD-WAN.

- Port 2 (ovs-lan).

  Этот порт используется для подключения к Linux-мосту.

- Порты 4800 и 4801 (sdwan0 и sdwan1).

  Для каждого WAN-порта создается VXLAN-порт. Первый VXLAN-порт имеет номер 4800. Другим VXLAN-портам присваиваются следующие по порядку номера. Например, второму VXLAN-порту присваивается номер 4801. В качестве IP-адреса источника требуется назначить IP-адрес соответствующего WAN-порта. Порту назначения нужно присвоить номер VXLAN-порта.

После того, как устройство CPE получает параметры WAN-портов по протоколу DHCP, на нем создаются отдельные таблицы маршрутизации для каждого из WAN-портов. Вы можете использовать шаблон CPE, чтобы указать следующие параметры портов:

- тип и конфигурация портов;
- количество внешних и внутренних портов;
- нумерация портов;
- действия, которые решение Kaspersky SD-WAN применяет к устройству CPE при его регистрации.

Для добавления шаблона CPE вам нужно перейти в раздел **SD-WAN** () веб-интерфейса оркестратора, после чего перейти в подраздел **CPE шаблоны конфигурации** ().

См. также

О шаблоне CPE.....35

Об устройствах uCPE

Вы можете установить программное обеспечение uCPE на сервер с архитектурой процессора x86. Устройство uCPE используется для построения сетей SD-WAN и дополнительно поддерживает развертывание VNF, как в виртуальной инфраструктуре ЦОД. В состав устройства uCPE входят гипервизор и VIM (Openstack в минимальной конфигурации). Остальные компоненты, необходимые для оркестрации VNF, находятся в ЦОД.

Оркестратор начинает взаимодействовать с VIM на устройстве uCPE после того, как это устройство регистрируется в инвентаризационной базе оркестратора и подключается к сервису управления SD-WAN managementTunnel, а также к другим SDN-сервисам. Сервис управления SD-WAN managementTunnel можно использовать для мониторинга работы устройства uCPE и настройки VNF.

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, в рамках которого развернут сервис SD-WAN. Вы можете выбрать другого тенанта, если вы используете один сервис SD-WAN для нескольких клиентов.

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 из списка устройств CPE, то все сервисные цепочки, развернутые на этом устройстве, будут удалены.

Все устройства uCPE имеют одинаковую логическую схему (см. рисунок ниже).

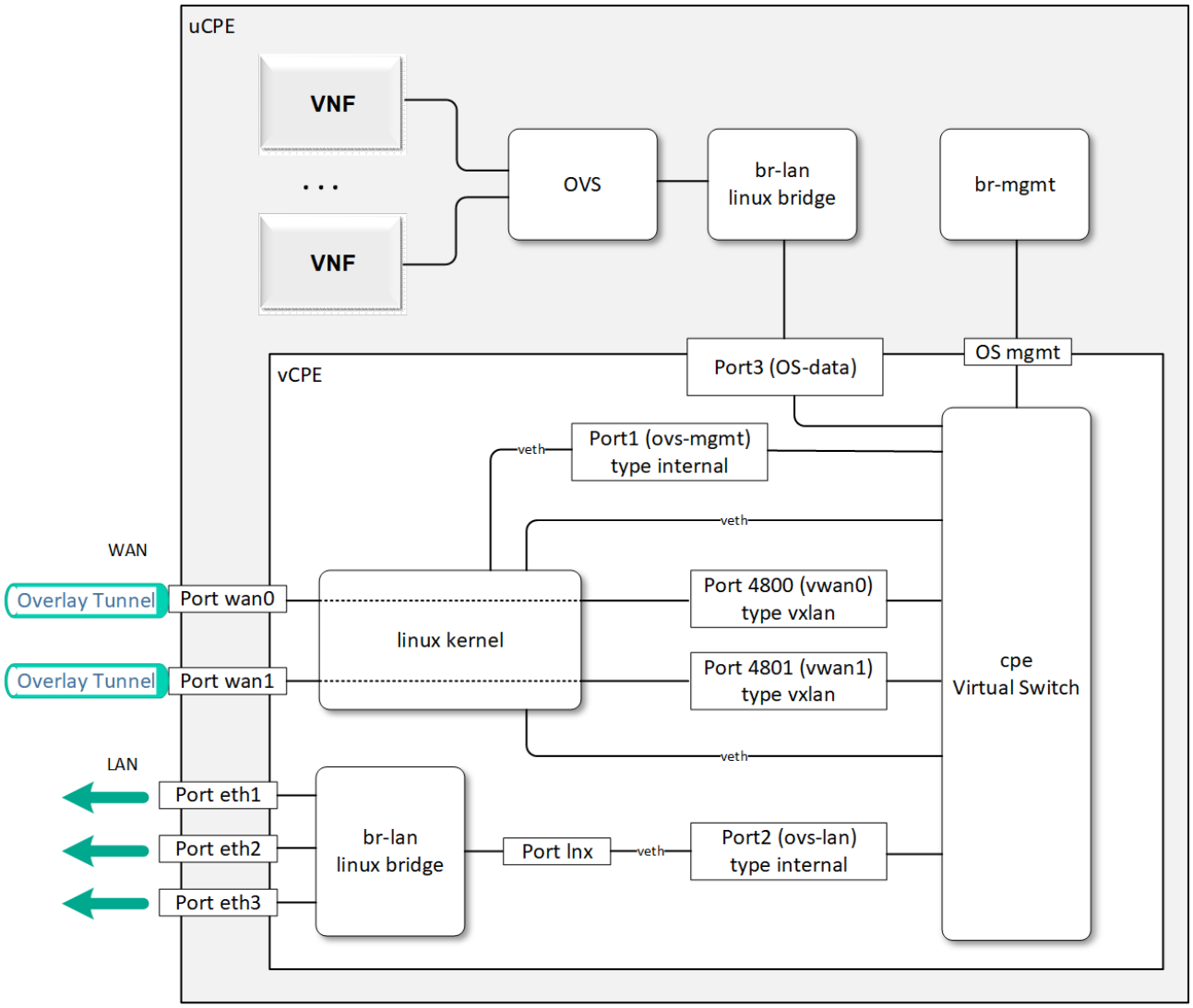

Рисунок 6. Логическая схема устройства uCPE

Программный коммутатор OpenFlow на устройстве uCPE содержит дополнительный порт OS-data. Вам нужно указать следующие номера портов OpenFlow в шаблоне uCPE:

- OS_Data – 3.
- Management – 1.
- LAN – 2.

  Если вы используете несколько LAN-портов, то вам нужно указать для них следующие по порядку номера. Например, для второго LAN-порта требуется указать номер 3.

Для добавления шаблона CPE вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора, после чего перейти в подраздел **CPE шаблоны конфигурации** ( ).

kaspersky

См. также

О шаблоне CPE

Шаблон CPE (англ. CPE template) содержит параметры устройства CPE. С помощью этого шаблона вы можете указать требуемые параметры устройства CPE, после чего применить их к нескольким устройствам.

Для создания шаблона CPE вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора, после чего перейти в подраздел **CPE шаблоны конфигурации** ( ). При создании шаблона CPE вам нужно указать тип устройства (CPE или uCPE), к которому шаблон будет применен. Чтобы настроить шаблон CPE, вы можете использовать вкладки, которые отображаются в верхней части области настройки шаблона CPE (см. таблицу ниже).

Таблица 8. Описание шаблона CPE

Вкладка	
Информация	На этой вкладке отображается название шаблона CPE. При создании шаблона CPE этому шаблону автоматически присваивается название. Если требуется, вы можете изменить название шаблона CPE по умолчанию.
Сопоставление портов	На этой вкладке вы можете установить соответствие между номерами OpenFlow-портов устройства CPE и их назначением. По умолчанию на этой вкладке добавлены следующие OpenFlow-порты: • OS_Data – 3. • Management – 1. • LAN – 2. Этот OpenFlow-порт добавляется только для шаблона uCPE. Мы не рекомендуем изменять порты по умолчанию, добавленные на этой вкладке.
Деактивация	На этой вкладке вы можете настроить функцию выключения устройства CPE и его удаления из инвентаризационной базы веб-интерфейса оркестратора. Решение Kaspersky SD-WAN использует эту функцию, когда на протяжении указанного времени отсутствует связь между устройством CPE и контроллером SD-WAN. Вы можете использовать эту функцию для предотвращения кражи устройств CPE или очистки инвентаризационной базы веб-интерфейса оркестратора от устаревших записей.
Шифрование	На этой вкладке вы можете настроить функцию шифрования трафика на устройстве CPE. Если требуется, вы можете включить или выключить эту функцию на отдельном наложенном туннеле.
Конфигурации	На этой вкладке вы можете добавить скрипты, которые решение Kaspersky SD-WAN запускает на устройстве CPE. Если для запуска скриптов требуются дополнительные файлы, то вы можете импортировать их в виде архива в формате TAR.GZ или ZIP. Архив должен содержать одну корневую папку, которая может включать в себя другие папки или файлы. После того, как решение регистрирует устройство CPE в оркестраторе, VNFM ожидает, когда устройство станет доступным через сервис управления SD-WAN managementTunnel, и запускает скрипты. Для обеспечения начального доступа к устройству CPE требуется указать имя пользователя и пароль по умолчанию, а также порт SSH. Позже указанные значения заменяются на автоматически сгенерированные значения. При добавлении скриптов вы можете выполнить следующие действия: • Выбрать исполнитель скрипта (англ. executor). Например, вы можете выбрать **Ansible**, **Expect** или **Custom**. • Выбрать статус устройства CPE, в котором требуется запустить скрипты. Например, вы можете запускать скрипты при регистрации устройства CPE. • Импортировать файл со скриптом или файл-сценарий Ansible playbook.
Мониторинг	На этой вкладке вы можете настроить способ мониторинга состояния устройства CPE. Мониторинг может осуществляться с помощью протокола SNMP или Zabbix-агентов. Вы также можете указать один из шаблонов мониторинга, созданных на сервере Zabbix.
Сервисы	На этой вкладке вы можете указать сервисы SD-WAN, чтобы устройство CPE автоматически подключилось к этим сервисам.

Консоли	На этой вкладке вы можете управлять доступом к консоли устройства CPE. Решение поддерживает подключение к веб-консоли устройства CPE, а также подключение к консоли по протоколу SSH.
VIM	На этой вкладке вы можете указать параметры для подключения оркестратора к VIM на устройстве uCPE. Этот раздел доступен, только если вы создаете шаблон для устройства uCPE. Устройства uCPE используют VIM для запуска виртуальных машин.

Вы можете привязать созданный шаблон к устройству CPE при добавлении этого устройства в список устройств CPE. Шаблоны CPE, привязанные к устройствам CPE, невозможно удалить. Чтобы отвязать шаблон от устройства CPE, требуется удалить это устройство.

См. также

Настройка устройств CPE 28

О списке устройств CPE 38

Операции с шаблонами CPE 37

Шифрование трафика 49

Операции с шаблонами CPE

Для выполнения операций с шаблонами CPE вам нужно перейти в раздел **SD-WAN** () веб-интерфейса оркестратора, после чего перейти в подраздел **CPE шаблоны конфигурации** (). Вы можете выполнять следующие операции с шаблонами CPE:

- Добавлять шаблоны CPE.

  Шаблон CPE используется для хранения параметров устройства CPE. При добавлении нового устройства в список устройств CPE вы можете применить к нему шаблон CPE. В этом случае все параметры, содержащиеся в шаблоне CPE, применяются к новому устройству CPE.

- Изменять шаблоны CPE.

  Обновленные параметры шаблона CPE не применяются к устройствам, которые уже были добавлены в список устройств CPE с применением этого шаблона.

- Удалять шаблоны CPE.

  Удаленные шаблоны CPE невозможно восстановить.

- Экспортировать шаблоны CPE.

  Когда вы экспортируете шаблон CPE, он загружается в вашу локальную систему в виде архива в формате TAR.GZ. Этот архив содержит XML-файл, описывающий шаблон CPE, файлы скриптов, а также файлы, используемые при выполнении скриптов, например SSL-сертификаты.
  В экспортированном шаблоне CPE не содержатся связи с тенантами.

- Импортировать шаблоны CPE.

  Чтобы импортировать шаблон CPE, вам нужно использовать архив в формате TAR.GZ или ZIP. Вы можете импортировать шаблон CPE целиком или выбрать отдельные вкладки, содержащие

требуемые параметры. Когда вы импортируете отдельные вкладки шаблона CPE, параметры на остальных вкладках шаблона остаются без изменений. Вам нужно импортировать шаблон CPE в один из добавленных шаблонов. Если к выбранному шаблону CPE привязаны устройства CPE, то они остаются привязанными к этому шаблону после того, как вы импортируете в него другой шаблон CPE и их параметры не обновляются. Вы также можете добавить новый шаблон CPE и импортировать в него существующий шаблон.

- Копировать шаблоны CPE.

  Решение копирует все вкладки шаблона CPE, а также добавленные скрипты и файлы. В скопированном шаблоне CPE не содержатся связи с тенантами и устройствами CPE.

- Просматривать список устройств, использующих шаблон CPE.

См. также

О шаблоне CPE.....35

О списке устройств CPE

Телекоммуникационное оборудование, которое будет подключаться к сервису SD-WAN, отображается в списке устройств CPE. Вам нужно добавить устройство в список устройств CPE перед отправкой на площадку. Для добавления устройства в список устройств CPE вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора. Этот раздел автоматически отображает подраздел **CPE инвентарь** ( ). При добавлении устройства в список устройств CPE вам нужно указать следующие параметры этого устройства:

- Уникальный идентификатор DPID.

  Идентификатор DPID привязывается к выбранному тенанту.

- Название устройства.

  Решение Kaspersky SD-WAN отображает название в списке устройств CPE.

- Адрес площадки, на которой будет находится устройство CPE.
- Шаблон CPE.

  Решение Kaspersky SD-WAN применяет к устройству параметры, которые указаны в выбранном шаблоне CPE.

- Тенант.

  Решение Kaspersky SD-WAN привязывает устройство CPE к выбранному тенанту.

Остальные параметры устройства CPE (IP-адрес, порт контроллера и шлюзов SD-WAN) указываются автоматически. Когда вы добавляете устройство в список устройств CPE, этому устройству присваивается статус *Ожидается*. После того, как устройство CPE подключается к оркестратору и получает необходимую информацию о конфигурации, статус устройства CPE меняется на *Регистрируется*. Если устройство CPE успешно подключается к контроллеру SD-WAN, то его статус меняется на *Зарегистрирован*.

Вы можете использовать список устройств CPE для просмотра параметров устройств (см. таблицу ниже).

Таблица 9. Параметры устройства CPE

Параметр	Описание
DPID	Уникальный идентификатор устройства CPE, который вы вводите при добавлении устройства в список устройств CPE. При регистрации устройство CPE передает свой идентификатор DPID оркестратору через API для сопоставления.
Модель	Модель устройства CPE. При регистрации устройство CPE передает информацию о своей модели оркестратору через API.
Версия SW	Версия программного обеспечения, установленного на устройстве CPE. При регистрации устройство CPE передает информацию о своем программном обеспечении оркестратору через API.
CPE шаблон	Шаблон CPE, который вы применили к устройству при добавлении в список устройств CPE.
Имя	Название устройства CPE. При добавлении устройства в список устройств CPE этому устройству автоматически присваивается название. Если требуется, вы можете изменить название устройства CPE по умолчанию.
Статус	Текущий статус устройства CPE. Каждое добавленное устройство CPE может иметь один из следующих статусов: • *Неизвестно*. Устройство CPE пытается подключиться к оркестратору, но идентификатор DPID этого устройства отсутствует в инвентаризационной базе оркестратора. • *Ожидание*. Устройство добавлено в список устройств CPE, но не подключено к оркестратору. • *Регистрация*. Устройство CPE находится в процессе регистрации. • *Ошибка*. В процессе регистрации устройства CPE возникла ошибка. • *Зарегистрировано*. Устройство CPE успешно зарегистрировано. • *Конфигурация*. На устройстве CPE применяются изменения параметров, внесенные пользователем.
Состояние	Состояние устройства CPE. После регистрации устройство CPE переходит в одно из следующих состояний: • Подключено. Устройство CPE активировано. • Отключено. Устройство CPE не активировано.
Подключение	Наличие или отсутствие подключения к устройству CPE в текущий момент.
Используется	Использование устройства CPE в сервисах SD-WAN. Если устройство CPE используется в сервисах SD-WAN, то его невозможно удалить.
Транспортный арендатор	Транспортный тенант, к которому привязано устройство CPE.

Параметр	Описание
Клиент-арендатор	Клиентский тенант, к которому привязано устройство CPE. Клиентом-арендатором может быть клиентская площадка или филиал вашего офиса.
Адрес	Адрес площадки, на которой расположено устройство CPE.
IP-адрес	IP-адрес устройства CPE в сети управления.
Контроллеры	Публичный IP-адрес и порт контроллера SD-WAN, которые используются для подключения устройства CPE и шлюзов SD-WAN, а также для взаимодействия устройства CPE с оркестратором.
Шлюзы	Публичные IP-адреса и порты шлюзов SD-WAN, которые используются для построения наложенных туннелей от устройства CPE, а также для взаимодействия устройства CPE с контроллером SD-WAN.
Мобильная сеть	Мобильные операторы, которые выпустили установленные в устройстве CPE SIM-карты.
Зарегистрировано	Дата и время регистрации устройства CPE.
Обновлено	Дата и время последнего изменения статуса устройства CPE.
Пользователь	Имя пользователя, который зарегистрировал устройство CPE.

Вы можете выбрать, параметры, которые отображаются в списке устройств CPE, отсортировать отображенные устройства CPE и найти устройство по одному из существующих параметров.

Когда вы добавляете устройство в список устройств CPE, на этом устройстве автоматически добавляются теги (метки). Эти теги отображают модель и версию программного обеспечения устройства CPE. Вы можете добавить собственные теги на устройствах CPE, чтобы классифицировать их для выполнения требуемых задач. Например, с помощью тегов вы можете сгруппировать устройства CPE, после чего обновить на них программное обеспечение.

См. также

О шаблоне CPE.....35

Операции с устройствами в списке устройств CPE.....40

Операции с устройствами в списке устройств CPE

Для выполнения операций с устройствами в списке устройств CPE вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора. Этот раздел автоматически отображает подраздел **CPE инвентарь** ( ). Вы можете выполнять следующие операции с устройствами в списке устройств CPE:

- Изменять параметры устройств CPE.
- Выключать устройства CPE.
- Удалять устройства CPE.

  При удалении устройства CPE соответствующий ему коммутатор удаляется из базы данных контроллера SD-WAN, устройство CPE отвязывается от тенанта и запись об этом устройстве

перестает отображаться в списке устройств CPE. Вы не можете удалить устройство CPE, которое используется в сервисах SD-WAN.

Доступность операций и параметры устройства CPE, которые вы можете изменить, зависят от статуса этого устройства CPE (см. таблицу ниже).

Таблица 10. Статусы устройств CPE и возможные операции

Статус устройства CPE	Возможные операции
Неизвестно	• Удаление устройства CPE. • Регистрация устройства CPE.
Ожидание	• Удаление устройства CPE. • Указание адреса площадки, на которой расположено устройство CPE.
Регистрация	Вы не можете выполнять операции с устройствами CPE в этом статусе.
Ошибка	Удаление устройства CPE.
Зарегистрировано	• Удаление устройства CPE. • Указание адреса площадки, на которой расположено устройство CPE. • Включение или выключение устройства CPE. • Просмотр пароля устройства CPE. • Отмена регистрации устройства CPE. • Открытие консоли устройства CPE. • Запуск скриптов на устройстве CPE. • Перезагрузка устройства CPE. • Отключение соединения с устройством CPE.
Конфигурация	• Указание адреса площадки, на которой расположено устройство CPE. • Просмотр пароля устройства CPE. • Открытие консоли устройства CPE.

См. также

О списке устройств CPE 38

Управление устройствами CPE

Для управления устройствами CPE и их мониторинга решение Kaspersky SD-WAN использует сервис управления SD-WAN managementTunnel. Корневым портом (англ. root port) является сервисный интерфейс с именем port 1 и типом инкапсуляции Access на основном шлюзе SD-WAN. Решение Kaspersky SD-WAN использует аналогичный порт на резервном шлюзе SD-WAN для создания резервного сервисного интерфейса.

После того, как устройство CPE подключается к контроллеру SD-WAN, оркестратор создает сервисный интерфейс на порту mgmt CPE с типом инкапсуляции Access. Вы можете указать номер этого порта в шаблоне CPE (по умолчанию порт имеет номер 1). Для настройки шаблона CPE вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора, после чего перейти в подраздел **CPE шаблоны**

конфигурации ( ). Оркестратор активирует устройство CPE и добавляет сервисный интерфейс в сервис управления SD-WAN managementTunnel с ролью Leaf (см. рисунок ниже).

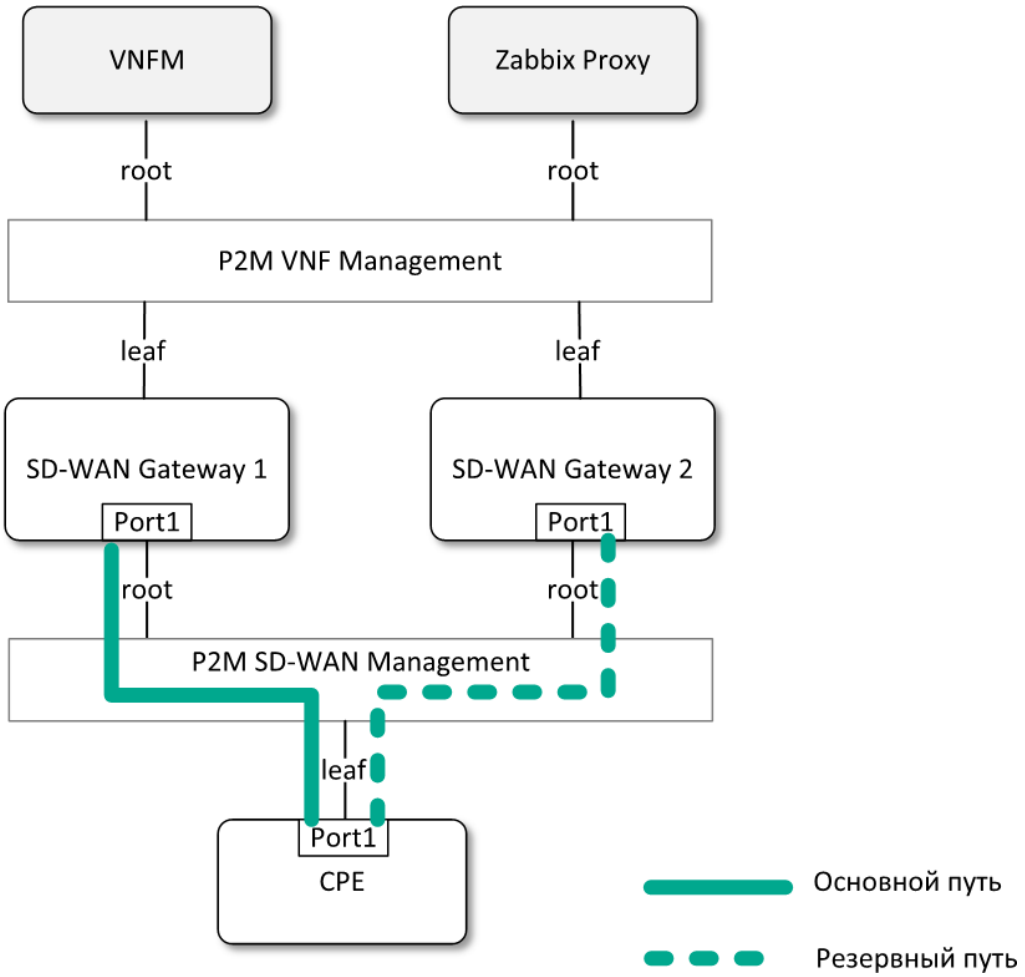

Рисунок 7. Сервис управления устройством CPE

IP-адрес, необходимый для управления устройством CPE, определяется автоматически из заданного вами пула адресов. Этот IP-адрес отображается в списке устройств CPE. 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. Для этого вам не нужно настраивать IP-связность с устройством CPE. VNFM предоставляет доступ к консоли через сервис управления SD-WAN managementTunnel.

См. также

kaspersky

Мониторинг устройств CPE

Для мониторинга устройств CPE решение использует внешнюю систему мониторинга Zabbix, которая состоит из серверов Zabbix и Zabbix Proxy. Сервера Zabbix Proxy устанавливаются в ЦОД и обеспечивают мониторинг отдельных устройств CPE, подключенных к сервису SD-WAN, который развернут в рамках ЦОД. Для сбора статистики сервер Zabbix Proxy использует сервис управления SD-WAN managementTunnel.

Мониторинг устройств CPE осуществляется с помощью Zabbix-агента или протокола SNMP. Вы можете выбрать способ мониторинга устройства при добавлении или изменении шаблона CPE на вкладке **Мониторинг**. Для настройки шаблона CPE вам нужно перейти в раздел **SD-WAN** () веб-интерфейса оркестратора, после чего перейти в подраздел **CPE шаблоны конфигурации** (). На вкладке **Мониторинг** вы также можете выбрать шаблон Zabbix (англ. Zabbix template), который вы создали на сервере Zabbix. *Шаблоны Zabbix* содержат графики, каждый из которых отображает результаты мониторинга одного из параметров устройства CPE, например процента использования центрального процессора.

После завершения процесса регистрации устройства CPE, когда устройство CPE подключается к контроллеру SD-WAN, на сервере Zabbix создается соответствующий хост для мониторинга этого устройства. Если вы удалите устройство из списка устройств CPE, то соответствующий этому устройству хост на сервере Zabbix также будет удален.

Чтобы просмотреть данные, полученные в ходе мониторинга устройства CPE, вам нужно нажать на устройство в списке устройств CPE и в области настройки устройства CPE выбрать вкладку **Мониторинг**. Вы можете выбрать один из доступных графиков, чтобы просмотреть результаты мониторинга требуемого параметра устройства CPE. Для каждого графика можно выбрать один из следующих временных интервалов отображения данных:

- В реальном времени.

  График отображает данные, полученные в течение последнего часа, и обновляется один раз в секунду.

- День.

  График отображает данные, полученные в течение последнего дня, и обновляется раз в день.

- Неделя.

  График отображает данные, полученные в течение последней недели, и обновляется раз в неделю.

- Месяц.

  График отображает данные, полученные в течение последнего месяца, и обновляется раз в месяц.

Вы можете настроить интервал отображения данных вручную.

См. также

О шаблоне CPE 35

О списке устройств CPE 38

kaspersky

Настройка протокола динамический маршрутизации BGP на устройствах CPE

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

Параметры использования протокола BGP указываются в области настройки шаблона CPE (см. раздел "О шаблоне CPE" на стр. 35) или отдельного устройства CPE на вкладке **BGP**. На этой вкладке отображаются следующие вкладки, которые вы можете использовать для настройки работы протокола BGP:

- **Глобальные**.

  На этой вкладке вы можете настраивать основные параметры использования протокола BGP на устройстве CPE. Например, вы можете указать номер вашей автономной системы, уникальный идентификатор устройства CPE (параметр router ID), а также временной интервал для отправки keep-alive сообщений.

- **Access Lists.**

  На этой вкладке вы можете настраивать списки управления доступом (англ. Access Control Lists, ACL) с IPv4-префиксами, которые затем можно использовать для фильтрации маршрутной информации на устройстве CPE.

- **Prefix Lists**.

  На этой вкладке вы можете настраивать списки префиксов (англ. prefix lists) с IPv4-префиксами и/или диапазонами IPv4-префиксов, которые затем можно использовать для фильтрации маршрутной информации на устройстве CPE. Диапазоны IPv4-префиксов указываются с помощью параметров Greater or Equal и Less or Equal.

- **Route Maps**.

  На этой вкладке вы можете настраивать карты маршрутизации (англ. route maps), также известные как политики маршрутизации, которые затем можно использовать для фильтрации и изменения атрибутов маршрутной информации.

- **Neighbors**.

  На этой вкладке вы можете указывать соседей устройства CPE, устанавливая TCP-соединение с другими устройствами CPE или сторонними сетевыми устройствами.

- **Peer Groups**.

  На этой вкладке вы можете указывать соседей устройства CPE, устанавливая динамическое TCP-соединение с другими устройствами CPE или сторонними сетевыми устройствами. В этом случае вам не нужно указывать параметры TCP-соединения для каждого отдельного соседа.

После того, как вы включаете использование протокола BGP в ходе настройки шаблона CPE, вам нужно применить этот шаблон к требуемым устройствам в списке устройств CPE (см. раздел "О списке устройств CPE" на стр. 38).

kaspersky

Управление трафиком

В этом разделе содержится информация о том, как настроить управление трафиком при построении сетей SD-WAN с помощью решения Kaspersky SD-WAN.

В этом разделе

Использование нескольких транспортных путей для передачи трафика

Решение Kaspersky SD-WAN поддерживает одновременное использование нескольких транспортных путей, подключенных к устройствам CPE, для передачи трафика (англ. multipathing) при построении сетей SD-WAN. Это повышает общую скорость подключения и доступность устройств CPE.

Контроллер SD-WAN воспринимает связность между двумя узлами сети как *сегмент*. Для настройки сегментов вам нужно перейти в раздел **Инфраструктура** ( ) веб-интерфейса оркестратора, открыть страницу настройки требуемого контроллера или узла контроллера SD-WAN, после чего перейти в раздел **Сегменты**. В этом разделе автоматически отображаются сегменты для каждой созданной вами связности между двумя узлами сети.

Каждый сегмент может содержать от 2 до 16 транспортных путей. Транспортные пути начинаются на начальном узле сегмента и заканчиваются на конечном узле сегмента. Вам нужно указать максимальное количество транспортных путей, поддерживаемых сегментами, при настройке контроллера SD-WAN. Если требуется, вы можете изменить максимальное количество транспортных путей для отдельного сегмента.

Транспортные пути имеют следующие параметры:

- Стоимость (англ. Path.cost).

  По умолчанию является суммой стоимости всех виртуальных каналов, которые входят в транспортный путь. Вы можете вручную определить стоимость определенных видов транспортных путей.

- Вес (англ. Path.weight).
- Тип (англ. Path.type).

  Решение Kaspersky SD-WAN поддерживает следующие типы транспортных путей:

  - Auto-SPF (Shortest-path forwarding).

Контроллер SD-WAN автоматически рассчитывает наилучший маршрут. Вы не можете создавать, изменять или удалять транспортные пути этого типа.

- Manual-TE (Traffic Engineering).

  Вы создаете транспортный путь вручную. Вам нужно указать все последовательные виртуальные каналы от начального до конечного узла сегмента.

- Auto-TE.

  Контроллер SD-WAN автоматически рассчитывает основной маршрут с применением указанных вами ограничений. Например, одним из таких ограничений может быть загруженность виртуального канала.

- Административное состояние (англ. Path.admin.state).

  Вам нужно указать значение параметра вручную. Если этот параметр имеет значение down, то транспортный путь не используется.

- Фактическое состояние (англ. Path.oper.state).

  Зависит от наличия или отсутствия возможности передачи трафика. Если этот параметр имеет значение down, то транспортный путь не используется.

Вам нужно указать параметры сегмента в шаблоне CPE, после чего применить этот шаблон к требуемым устройствам CPE. Для настройки шаблонов CPE вам нужно перейти в раздел **SD-WAN** () веб-интерфейса оркестратора, после чего перейти в подраздел **CPE шаблоны конфигурации** ().
При изменении параметров отдельного устройства в списке устройств CPE вы также можете указать параметры сегмента. Для настройки устройства CPE вам нужно перейти в раздел **SD-WAN** () веб-интерфейса оркестратора. Этот раздел автоматически отображает подраздел **CPE инвентарь** ().

Вы можете изменить следующие параметры сегмента:

- Указать максимальное количество транспортных путей в поле **Максимальное кол-во путей**.
- Указать максимальное количество транспортных путей типа Auto-SPF в поле **Maximum number of Auto-SPF paths**.
- Указать коэффициент в поле **Cost variance multiplier**.

  Этот коэффициент определяет, во сколько раз больше может быть стоимость транспортного пути по сравнению с наилучшим маршрутом, чтобы этот транспортный путь мог быть добавлен в сегмент. Вы можете ввести значения от 1 до 10.

- Установить флажок **Enable Multi Weight**.

  Если вы установили этот флажок, то трафик распределяется по транспортным путям сегмента приблизительно пропорционально значению параметров веса (англ. Path.weight). Вы можете снять этот флажок, чтобы трафик распределяется равномерно и параметр веса для всех транспортных путей был равен 1.

См. также

Создание транспортных сервисов, соответствующих SLA

Решение Kaspersky SD-WAN поддерживает создание транспортных сервисов, соответствующих соглашениям об уровне сервиса (англ. Service Level Agreement, далее также SLA). Для создания таких транспортных сервисов вы можете использовать ограничения (англ. constraints). *Ограничения* определяют, как трафик маршрутизируется через виртуальные каналы, соединяющие устройства CPE и шлюзы SD-WAN в рамках транспортного сервиса. При использовании SLA маршрутизация зависит от показателей мониторинга на виртуальных каналах. Чтобы создать транспортный сервис, соответствующий SLA, вам нужно выполнить следующие шаги:

1. Включить мониторинг виртуальных каналов и установить пороговые значения показателей мониторинга.
2. Создать требуемые ограничения.
3. Указать созданные ограничения в параметрах требуемого транспортного сервиса.

Для включения мониторинга виртуальных каналов на устройстве CPE вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратор. Этот раздел автоматически отображает подраздел **CPE инвентарь** ( ). Затем вам потребуется нажать на устройство в списке устройств CPE и в области настройки выбрать вкладку **Туннели**. На этой вкладке вы можете включить мониторинг для требуемого виртуального канала и указать параметры мониторинга (см. таблицу ниже).

Таблица 11. Описание параметров мониторинга

Параметр	Описание
Нежелательный	Вы можете установить этот флажок, чтобы отметить виртуальный канал как нежелательный. *Нежелательные* виртуальные каналы не используются при маршрутизации или используются в последнюю очередь, независимо от качества связи.
Интервал обработки ошибок линка и статистики использования, сек	Интервал для измерения процента ошибок на виртуальном канале и уровня его загруженности. Интервал указывается в секундах. Вы можете ввести значение от 1 до 300.
Уровень критических ошибок линка, ошибок/сек	Пороговое значение уровня ошибок на виртуальном канале. Вы можете ввести значение от 1 до 1 000 000.
Критический уровень использования линка, %	Пороговое значение загруженности виртуального канала в процентах от установленной скорости сервисного интерфейса. Вы можете ввести значение от 50 до 100.
Качество связи (задержка, джиттер, потеря пакетов), интервал обработки статистики	Интервал для измерения показателей задержки (англ. latency), вариации задержки (англ. jitter) и потери пакетов (англ. packet loss). Интервал указывается в секундах. Вы можете ввести значение от 1 до 600.
Критический уровень задержек линка, сек	Максимально допустимое время задержки при передаче пакетов в миллисекундах. Вы можете ввести значение от 5 до 1000.
Критический уровень джиттера линка, мсек	Максимально допустимое время вариации задержки в миллисекундах. Вы можете ввести значение от 5 до 1000.
Критический уровень потерь пакетов линка, %	Максимально допустимый процент потери пакетов. Вы можете ввести значение от 1 до 100.

Скорость сервисного интерфейса может не соответствовать реальной полосе виртуального канала. В этом случае для мониторинга загрузки полосы вам нужно вручную указать скорость сервисного интерфейса в параметрах контроллера SD-WAN.

Виртуальные каналы, для которых включен мониторинг, используются при создании ограничений. Если один из показателей мониторинга на виртуальном канале достигает порогового значения, то при построении транспортного пути типа Auto-TE решение Kaspersky SD-WAN в зависимости от параметров ограничения по возможности или гарантировано обходит этот виртуальный канал.

Для создания ограничений вам нужно перейти в раздел **Инфраструктура** () веб-интерфейса оркестратора, открыть страницу настройки требуемого контроллера или узла контроллера SD-WAN, после чего перейти в раздел **Ограничения**. При создании ограничения вам нужно выбрать показатели мониторинга, которые решение Kaspersky SD-WAN будет учитывать при выборе виртуального канала. Вы можете использовать флажок **Ignore** справа от требуемого показателя мониторинга, чтобы определить, как

осуществляется передача трафика в случае, если решение Kaspersky SD-WAN не обнаруживает альтернативных виртуальных каналов, соответствующих ограничению. Если вы установили этот флажок, трафик передается дальше, даже если виртуальный канал не соответствует ограничению. Чтобы отменить передачу трафика в таких случаях, вам нужно снять флажок.

После того, как вы создаете ограничение, оно отображается в разделе **Ограничения** вместе с выбранными показателями мониторинга. Показатели мониторинга могут иметь следующие статусы:

- *Y*.

  При достижении порогового значения по этому показателю на виртуальном канале этот виртуальный канал не будет использоваться.

- *Y I*.

  При достижении порогового значения по этому показателю на виртуальном канале и отсутствии альтернативных виртуальных каналов, соответствующих ограничению, этот виртуальный канал будет использоваться.

- *N*.

  Этот показатель не учитывается при маршрутизации.

Вы можете выбрать созданное ограничение при создании транспортного сервиса, который должен соответствовать SLA. Для создания транспортного сервиса вам нужно перейти в раздел **Инфраструктура** ( ) веб-интерфейса оркестратора, открыть страницу настройки контроллера или узла контроллера SD-WAN, после чего перейти в раздел требуемого транспортного сервиса, например в раздел **P2P сервисы**. Маршрутизация в рамках созданного транспортного сервиса будет осуществляться с учетом параметров наложенного ограничения.

См. также

О шаблоне CPE.....35

О списке устройств CPE.....38

Шифрование трафика

Шифрование трафика – это механизм, обеспечивающий безопасную передачу трафика между устройствами CPE через наложенные туннели. В рамках сети SD-WAN, построенной с помощью решения Kaspersky SD-WAN, вы можете использовать шифрование трафика при передаче данных между устройствами CPE по незащищенному каналу связи через интернет.

Контроллер SD-WAN создает ключи для шифрования и дешифровки трафика и передает его на требуемые устройства CPE. Трафик шифруется на устройстве CPE-отправителе с помощью ключа для шифрования перед передачей на наложенный туннель. Устройство CPE-получатель принимает трафик из наложенного туннеля и дешифрует его с помощью ключа для дешифровки.

Чтобы исключить возможность дешифровки переданного трафика третьими лицами при перехватывании ключа, используемые ключи регулярно обновляются. Вы можете указать время, которое проходит между обновлениями ключей на устройствах CPE, изменив значение параметра контроллера SD-WAN topology.link.encryption.key.update.interval.minutes (см. раздел "Настройка параметров контроллера SD-WAN" на стр. 25).

Шифрование трафика поддерживается только на устройствах CPE с программным обеспечением Kaspersky SD-WAN.

Функция шифрования трафика может быть по умолчанию включена или выключена на устройстве CPE в зависимости от шаблона CPE, примененного к этому устройству. Вы можете настроить функцию шифрования трафика на отдельном устройстве CPE. Для этого вам нужно нажать на устройство в списке устройств CPE и в области настройки устройства CPE выбрать вкладку **Шифрование**.

Если вы включаете функцию шифрования трафика на устройстве CPE, то все исходящие наложенные туннели, связанные с этим устройством, начинают передавать зашифрованный трафик. Новые исходящие наложенные туннели, построенные с использованием этого устройства CPE, также будут передавать зашифрованный трафик.

Когда вы выключаете шифрование трафика на устройстве CPE, ключи, которые контроллер SD-WAN создал для шифрования и дешифровки трафика, удаляются со всех задействованных устройств CPE.

Решение Kaspersky SD-WAN поддерживает включение и выключение функции шифрования трафика на отдельных наложенных туннелях. Например, вы можете включить шифрование трафика на устройстве CPE, но выключить его на отдельном наложенном туннеле, который создан с использованием этого устройства CPE. При включении или выключении шифрования трафика на наложенном туннеле вам нужно одинаковым образом настроить как исходящий, так и входящий наложенные туннели.

См. также

О шаблоне CPE 35

О списке устройств CPE 38

Фильтрация трафика

В этом разделе содержится информация о настройке параметров фильтрации трафика. Вы можете фильтровать трафик для обеспечения безопасности сети SD-WAN и ее соответствия SLA, а также для классификации интересующего вас трафика и его последующего зеркалирования (англ. port mirroring).

В этом разделе

Создание правил классификации трафика 50

Создание фильтров трафика 53

Маршрутизация трафика по приложениям 55

Создание правил классификации трафика

Вы можете создавать правила классификации трафика для определения классов трафика и последующего управления этими классами. Для создания правил классификации трафика вам нужно перейти в раздел

Инфраструктура ( ) веб-интерфейса оркестратора, открыть страницу настройки требуемого контроллера или узла контроллера SD-WAN, после чего перейти в раздел **Фильтр**. В этом разделе выберите вкладку **Правила**. Правила классификации трафика относят пакеты трафика к разным классам по значениям полей заголовков уровней L2-L4 (см. таблицу ниже).

Таблица 12. Описание полей заголовков разных уровней и возможных значений

Поле заголовка	Возможные значения
Заголовки уровня L2	
Outer VLAN id	0–4095.
Outer VLAN pcp	0–7.
MAC источника	00:00:00:00:00:00 – ff:ff:ff:ff:ff:ff.
Маска MAC источника	
MAC назначения	
Маска MAC назначения	
Ethertype	Вы можете выбрать одно из следующих значений в раскрывающемся списке: • **0x0800**. Это значение выбрано по умолчанию. • **0x86dd**. • **0x0806**.
Заголовки уровня L3	
Протокол	Вы можете выбрать одно из следующих значений в раскрывающемся списке: • **IPv4**. Это значение выбрано по умолчанию. • **IPv6**. Вам нужно выбрать значение в этом раскрывающемся списке, чтобы использовать значения полей заголовков уровня L4 при создании правил классификации трафика.
IP источника	Для протокола IPv4: 0.0.0.0 – 255.255.255.255. Для протокола IPv6: 0000:0000:0000:0000:0000:0000:0000:0000 – ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
Длина префикса IP источника	Для протокола IPv4: /0 – /32. Для протокола IPv6: /0 – /128.
IP назначения	Для протокола IPv4: 0.0.0.0 – 255.255.255.255. Для протокола IPv6: 0000:0000:0000:0000:0000:0000:0000:0000 – ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
Длина префикса IP назначения	Для протокола IPv4: /0 – /32. Для протокола IPv6: /0 – /128.

Поле заголовка	Возможные значения
DSCP	Вы можете выбрать одно из значений в раскрывающемся списке. Вы не можете использовать это поле заголовка совместно с полем заголовка **TOS** в одном правиле классификации трафика.
TOS	0–255. Вы не можете использовать это поле заголовка совместно с полем заголовка **DSCP** в одном правиле классификации трафика.
Заголовки уровня L4	
IP протокол	Вы можете выбрать одно из следующих значений в раскрывающемся списке: • **TCP**. Это значение выбрано по умолчанию. • **UDP**. • **ICMP**. • **Other**. Если вы выбрали это значение, то вам становится доступно поле **Number**. В этом поле вы можете ввести значения в диапазоне 0–255.
Список портов источника	0–65535. Вы можете ввести номера нескольких портов через запятую или указать диапазон значений с помощью тире.
Список портов назначения	
Номер типа ICMP	0–255. Вы можете ввести только одно значение.

Вы можете классифицировать пакеты трафика на основании приложений, которые их отправляют. На вкладке **DPI** отображается раскрывающийся список **Application** для выбора приложения. Когда вы выбираете приложение, внутренняя метка, которой устройства CPE будут маркировать его трафик отображается в поле **PKT Mark**.

Правила классификации трафика могут содержать несколько условий, которые будут суммироваться друг с другом с использованием логического оператора AND.

См. также

Создание фильтров трафика

Фильтр трафика – это группа правил классификации трафика, в которой каждое правило имеет приоритет и выполняет определенное действие с трафиком (разрешает или запрещает маршрутизацию трафика).

Для создания фильтров трафика вам нужно перейти в раздел **Инфраструктура** ( ) веб-интерфейса оркестратора, открыть страницу настройки требуемого контроллера или узла контроллера SD-WAN, после

чего перейти в раздел **Фильтры**. При создании фильтра трафика вам нужно указать его параметры (см. таблицу ниже).

Таблица 13. Описание параметров фильтра трафика

Параметр	Описание
Имя	Название фильтра трафика. Это название отображается на вкладке **Фильтры** после создания фильтра трафика.
Последовательность	Порядковый номер правила классификации трафика, которое вы добавляете в фильтр трафика. Вы можете ввести номер в диапазоне 1–998. Правило с наименьшим номером в поле **Последовательность** имеет наибольший приоритет.
Правило	Правило классификации трафика. Вы можете выбрать одно из созданных правил классификации трафика в раскрывающемся списке.
Действие	Действие, которое выбранное правило классификации трафика применяет к трафику. Вы можете выбрать одно из следующих значений: • **Permit**. При срабатывании правило разрешает последующую маршрутизацию трафика. • **Deny**. При срабатывании правило запрещает последующую маршрутизацию трафика
Добавить	Вы можете нажать на эту кнопку, чтобы добавить правило классификации трафика в фильтр трафика.
Удалить	Вы можете нажать на эту кнопку, чтобы удалить правило классификации трафика из фильтра трафика.
Действие по умолчанию	Правило классификации трафика с наиболее низким приоритетом. Это правило классификации трафика применяется к трафику, который не соответствует ни одному из добавленных правил.

При создании транспортного сервиса вы можете выбрать один из созданных фильтров трафика в поле **Inbound Filter**. Для создания транспортного сервиса вам нужно перейти в раздел **Инфраструктура** ( ) веб-интерфейса оркестратора, открыть страницу настройки требуемого контроллера или узла контроллера SD-WAN, после чего перейти в раздел требуемого транспортного сервиса, например в раздел **P2P сервисы**.

См. также

Создание правил классификации трафика 50

Обработка трафика приложений

Программные коммутаторы OpenFlow по умолчанию не обрабатывают трафик выше 4-го уровня сетевой модели OSI (англ. Open Systems Interconnection model), в связи с чем обработка трафика приложений,

который находится на 7-м уровне, становится невозможной. Для обеспечения обработки трафика приложений решение Kaspersky SD-WAN использует технологию DPI (deep packet inspection).

Технология DPI осуществляет полный анализ передаваемых пакетов и их полезной нагрузки (англ. payload), в отличии от стандартных брандмауэров, которые анализируют только данные, содержащиеся в заголовках пакетов, такие как IP-адрес и порт отправителя или получателя.

Программное обеспечение Kaspersky SD-WAN, установленное на устройствах CPE анализирует передаваемые пакеты с помощью технологии DPI, распознает трафик приложений и маркирует его специальной внутренней меткой (PKT mark). Вы можете использовать эту метку для выделения трафика отдельных приложений с помощью правил классификации трафика и создания фильтров трафика. Например, вы можете создать отдельные правила классификации трафика для приложений, работающих по технологии унифицированных коммуникаций (англ. Unified Communications, UC), после чего направить трафик этих приложений в требуемый сервис SD-WAN через сервисные интерфейсы с помощью фильтра трафика.

В ходе обработки трафика приложений технология DPI также обеспечивает его мониторинг, предоставляя вам информацию не только о том, какое приложение передает трафик, но и о количестве передаваемого трафика. Для просмотра результатов мониторинга вам нужно перейди в раздел **SD-WAN** ( ) веб-интерфейса оркестратора и в подразделе **CPE инвентарь** ( ) нажать на устройство CPE, через которое осуществляется маршрутизация трафика требуемого приложения. На вкладке **Мониторинг** вы можете выбрать приложение и отобразить результаты мониторинга его трафика в виде графика.

См. также

Создание правил классификации трафика 50
Создание фильтров трафика 53

Маршрутизация трафика по приложениям

Вы можете использовать фильтры трафика для определения трафика критичных приложений и последующей балансировки этого трафика с учетом требований SLA. Для этого вам нужно выполнить следующие действия:

- включить режим использования нескольких транспортных путей для передачи трафика;
- создать ограничения для трафика;
- создать фильтры трафика;
- создать транспортный сервис и указать требуемые сервисные интерфейсы с типом инкапсуляции Access, VLAN или QinQ.

Затем вам нужно создать сервисные интерфейсы ACL (Access Control List). Для создания сервисных интерфейсов ACL вам нужно перейти в раздел **Инфраструктура** ( ) веб-интерфейса оркестратора, открыть страницу настройки требуемого контроллера или узла контроллера SD-WAN, после чего перейти в раздел **Сервисные интерфейсы**. Сервисные интерфейсы ACL создаются поверх стандартных сервисных интерфейсов. Чтобы создать сервисный интерфейс ACL, вам нужно выбрать фильтр трафика, который будет обрабатывать трафик и маршрутизировать его в транспортный сервис. При создании сервисного интерфейса ACL вам нужно указать его параметры (см. таблицу ниже).

Таблица 14. Описание параметров сервисного интерфейса ACL

Параметр	Описание
Type	Тип сервисного интерфейса. Для создания сервисного интерфейса ACL вам нужно выбрать **ACL** в раскрывающемся списке.
Underlay SI	Стандартный сервисный интерфейс, поверх которого создается сервисный интерфейс ACL. Чтобы удалить стандартный сервисный интерфейс, вам нужно удалить все сервисные интерфейсы ACL, созданные поверх него.
Filter	Фильтр трафика, который используется на сервисном интерфейсе ACL. Вы можете использовать один фильтр трафика на нескольких стандартных сервисных интерфейсах.
Match order	Порядок обработки трафика на сервисном интерфейса ACL. Вы можете выбрать один из пяти порядков обработки трафика (**Match order 1**–**5**) в раскрывающемся списке. Если вы выбираете порядок обработки трафика для сервисного интерфейса ACL, то это значение невозможно выбрать для других сервисных интерфейсов ACL, созданных поверх выбранного стандартного сервисного интерфейса.
Описание	Краткое описание сервисного интерфейса ACL.

На рисунке ниже отображены транспортные сервисы, которые имеют следующие характеристики:

- Сервисный интерфейс Underlay SI добавлен в стандартный транспортный сервис, к которому не применены ограничения.

  В этот транспортный сервис попадает весь трафик, который отбрасывается фильтрами трафика, примененными к двум другим транспортным сервисам (отмечены голубым и красным цветом).

- Сервисный интерфейс ACL SI 1 принадлежит к транспортному сервису, отмеченному синим цветом, и имеет ограничение по задержке входящих пакетов.

  В этот транспортный сервис маршрутизируется чувствительный к задержкам трафик.

- Сервисный интерфейс ACL SI 2 принадлежит к транспортному сервису, отмеченному красным цветом, и имеет ограничение по доступной полосе пропускания.

  В этот транспортный сервис маршрутизируется чувствительный к полосе пропускания трафик.

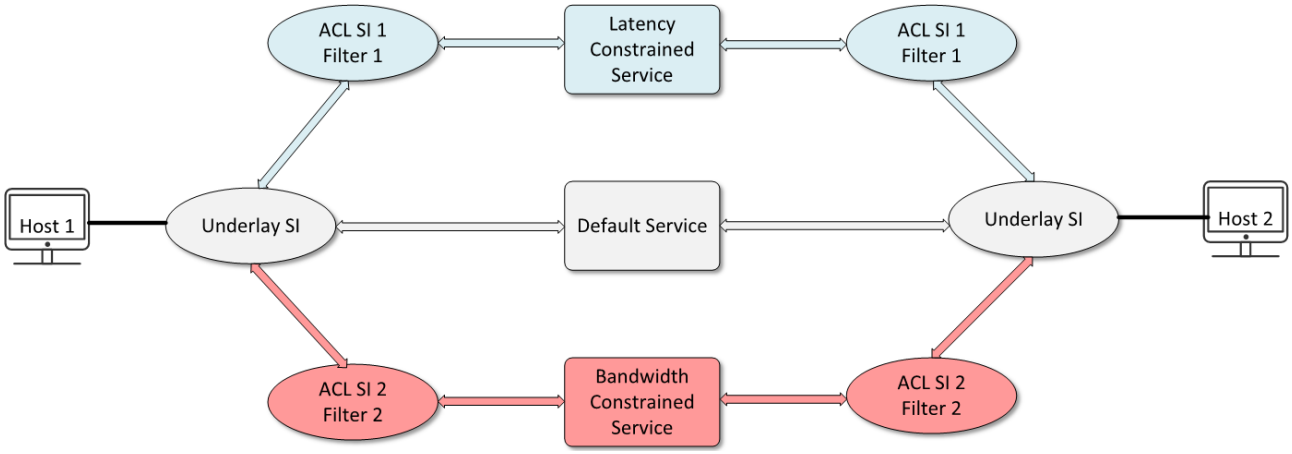

Рисунок 8. Схема маршрутизации трафика по приложениям с учетом SLA

Вам нужно указать созданные сервисные интерфейсы ACL при создании транспортного сервиса, после чего применить к этому транспортному сервису созданные ограничения. Для создания транспортного сервиса

вам нужно перейти в раздел **Инфраструктура** ( ) веб-интерфейса оркестратора, открыть страницу настройки контроллера или узла контроллера SD-WAN, после чего перейти в раздел требуемого транспортного сервиса, например в раздел **P2P сервисы**.

См. также

kaspersky

Резервирование и отказоустойчивость

В этом разделе содержится информация о резервировании компонентов сети SD-WAN и обеспечении их отказоустойчивости.

Решение Kaspersky SD-WAN поддерживает работу сети SD-WAN, когда возникают следующие виды сбоев:

- Отказ одного из центральных компонентов.

  Например, сеть SD-WAN сохраняет работоспособность при отказе оркестратора, шлюза или контроллера SD-WAN.

- Отказ или перегрузка каналов связи между центральными компонентами при их георезервировании.

  Георезервирование – это размещение компонентов сети на географически разнесенных площадках для обеспечения надежности хранения данных.

- Отказ или перегрузка каналов связи между устройствами CPE и шлюзами SD-WAN.

В этом разделе

Резервирование центральных компонентов решения

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

Таблица 15. Схемы резервирования компонентов сети SD-WAN

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	VXLAN (DTLS)

На рисунке ниже представлен пример размещения компонентов сети SD-WAN в географически разнесенных ЦОД. На всех рисунках ниже используются следующие условные обозначения:

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

- шлюз SD-WAN – GW.

Для компонентов сети SD-WAN, 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.

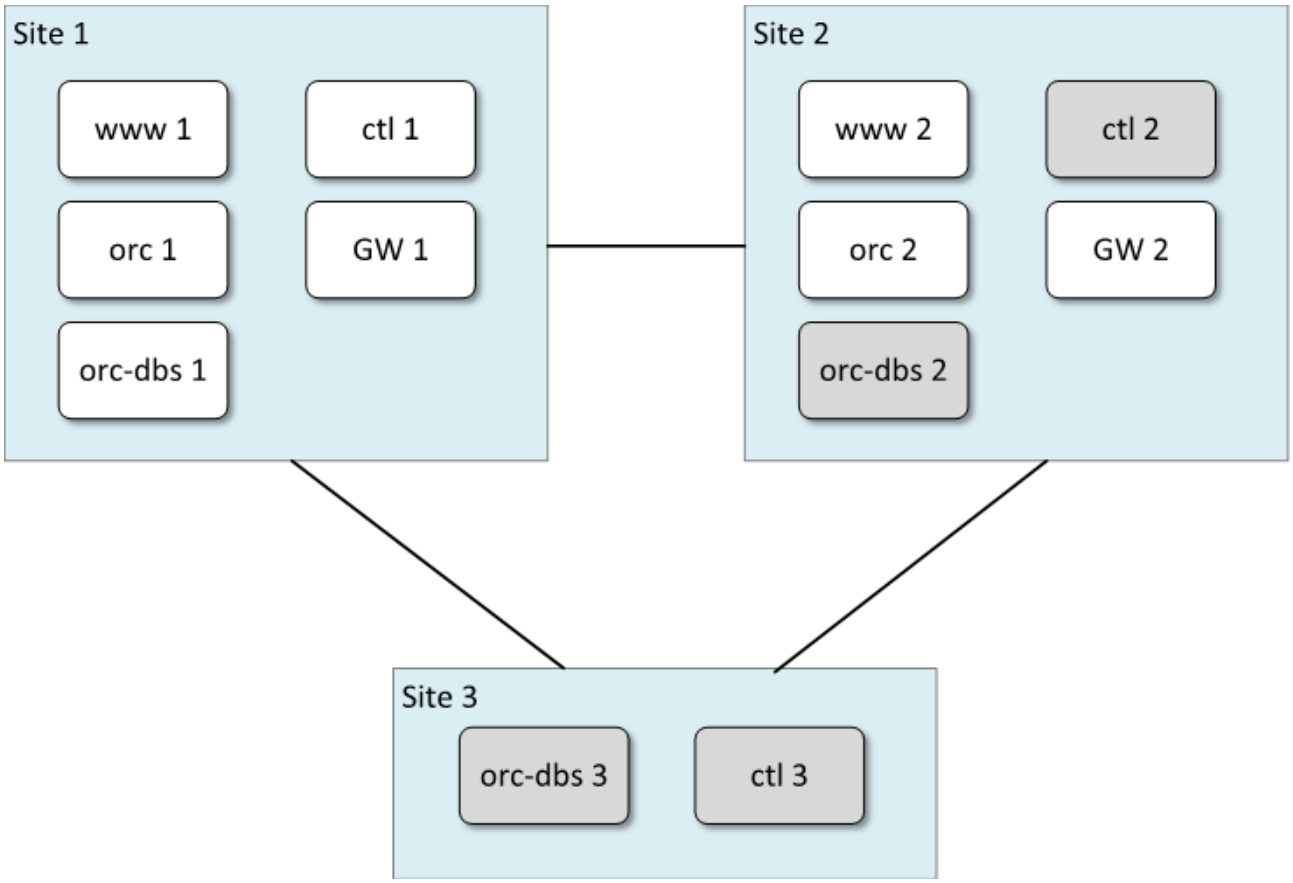

Рисунок 9. Размещение компонентов сети SD-WAN в географически разнесенных ЦОД

Компоненты, которые резервируются по схеме 2N+1 образуют кластер. Этот кластер содержит один главный узел и два второстепенных узла. Вы можете назначить один из узлов арбитром для экономии ресурсов и снижения требований к каналам связи. Если узел кластера назначен арбитром, то он не содержит базу данных, и вы не можете сделать его главным узлом. Узел-арбитр участвует в голосовании при выборе главного узла и обменивается с другими узлами периодическими служебными пакетами (англ. heartbeats).

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

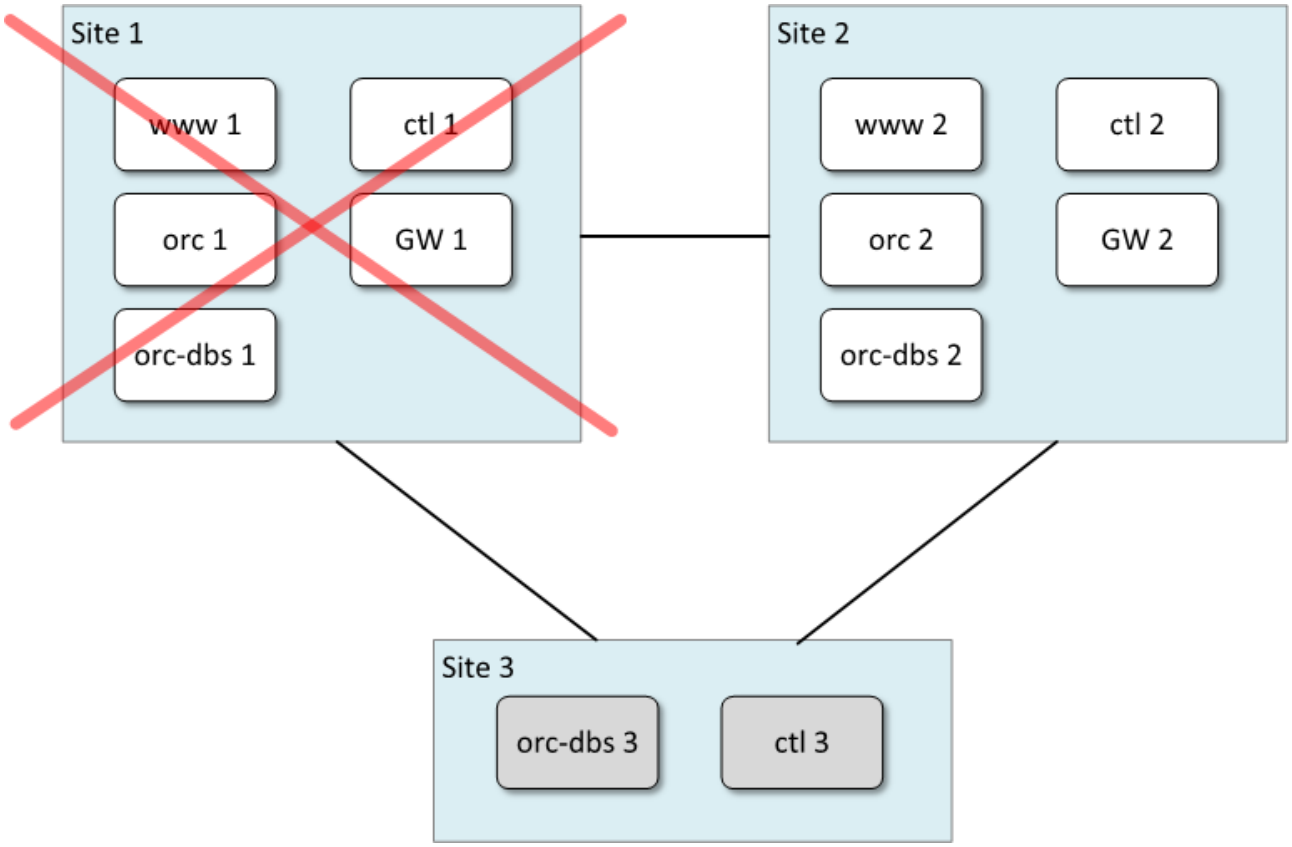

Рисунок 10. Авария на площадке 1

Если узлы кластера компонентов сети SD-WAN на площадке 1 выходят из строя, то происходят следующие события:

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

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

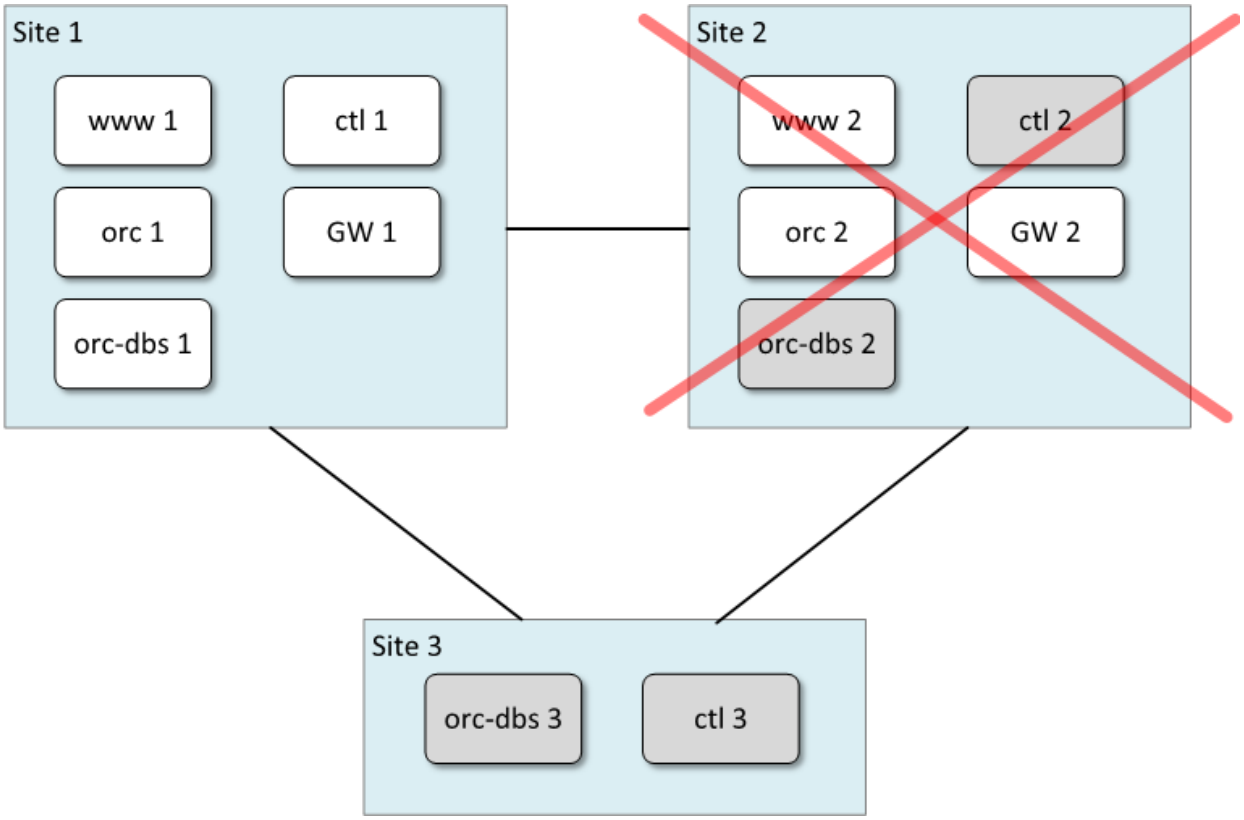

Рисунок 11. Авария на площадке 2

Если узлы кластера компонентов сети SD-WAN на площадке 2 выходят из строя, то происходят следующие события:

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

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

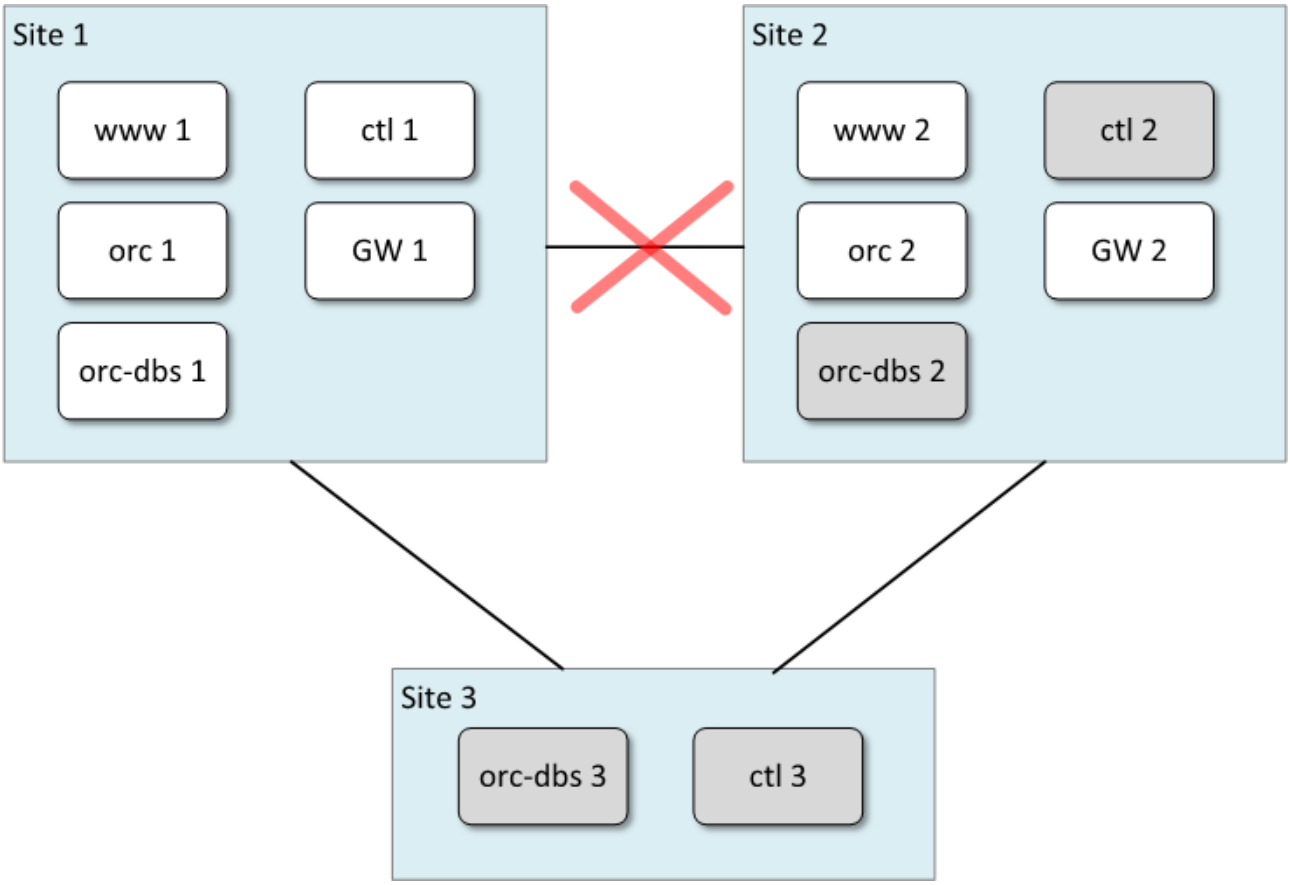

Рисунок 12. Авария на соединении между площадками 1 и 2

Если узлы кластера компонентов сети SD-WAN на площадках 1 и 2 не могут установить соединение друг с другом, то происходят следующие события:

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

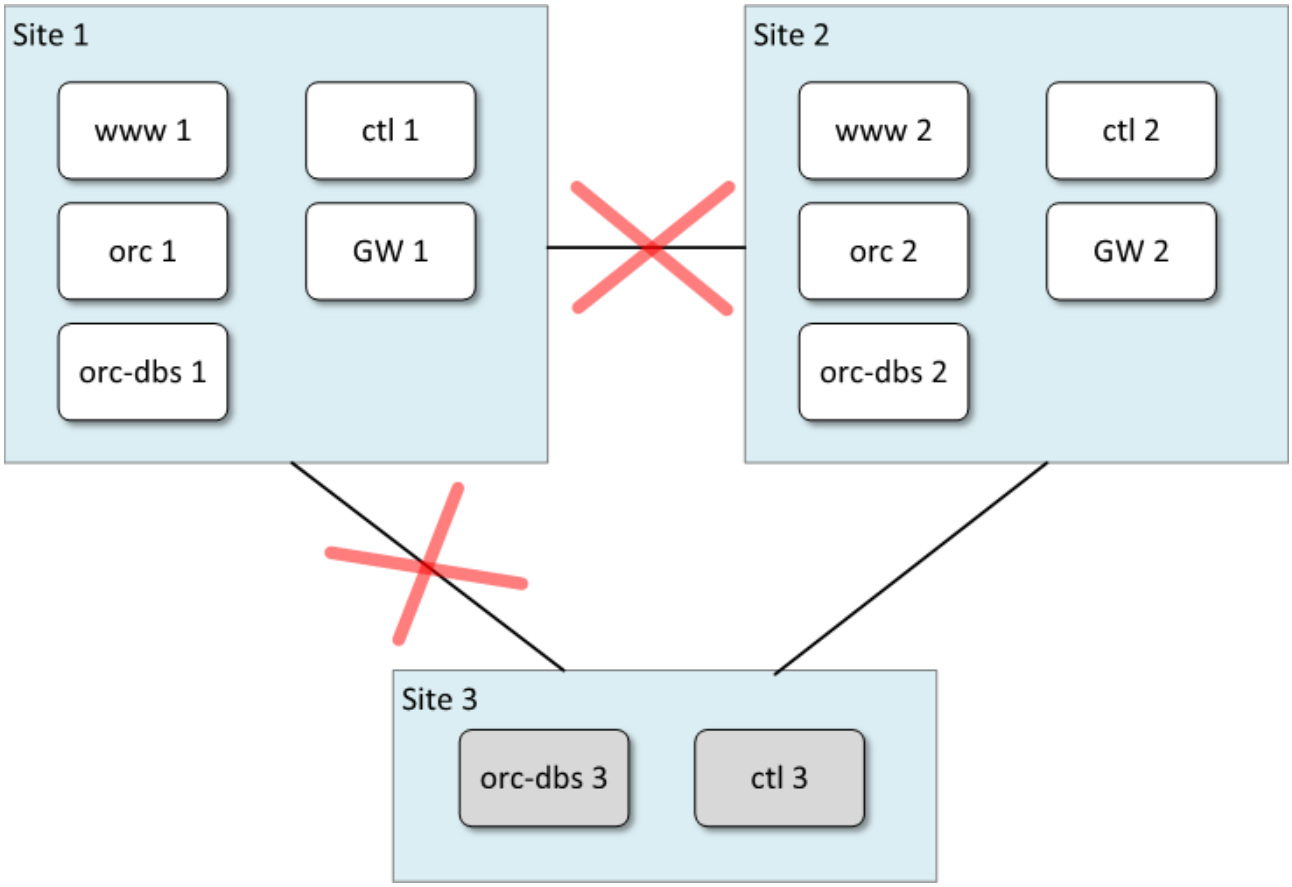

Рисунок 13. Авария на соединениях между площадкой 1 и остальными площадками

Если узлы кластера компонентов сети SD-WAN на площадке 1 не могут установить соединение с остальными площадками, то происходит следующие события:

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

О резервировании каналов связи с устройствами CPE

Решение обеспечивает защиту от перерывов связи с устройствами CPE с помощью одновременного использования всех доступных каналов, например интернет- или LTE-каналов. Поддерживаются два режима резервирования каналов связи с устройствами CPE – Active/Active и Active/Standby.

Режим резервирования каналов связи Active/Active

В этом режиме все WAN-порты устройств CPE находятся в активном состоянии и используются для передачи трафика пользователей. Контроллер SD-WAN обеспечивает балансировку трафика

с использованием нескольких транспортных путей (англ. multipathing). Вы можете использовать от 2 до 16 транспортных путей. Балансировка происходит на сессионном уровне с учетом информации на уровнях L2–L4. Вы можете использовать следующие типы балансировки:

- Эквивалентная балансировка.

  Вес каждого транспортного пути равен 1. Трафик равномерно распределяется по транспортным путям.

- Неэквивалентная балансировка.

  Трафик распределяется по транспортным путям примерно пропорционально их весу.

В режиме Active/Active устройство CPE остается доступным, пока сохраняется работоспособность хотя бы одного канала связи.

Режим резервирования каналов связи Active/Standby

В этом режиме вам нужно выбрать основной и резервный транспортный путь для передачи трафика. Для этого вам потребуется ввести значение `1` в поле **Maximum number of Auto-SPF paths** в области настройки требуемого устройства CPE, на вкладке **Multipathing**. В этом случае решение будет использовать один наложенный туннель для передачи трафика. Вам также нужно уменьшить цену основного наложенного туннеля по сравнению с резервным в области настройки требуемого устройства CPE на вкладке **Туннели**. Наложенные туннели являются однонаправленными, поэтому требуется аналогично изменить цену обратного наложенного туннеля. Контроллер SD-WAN автоматически вычисляет цену всех возможных наложенных туннелей и выбирает туннель с наименьшей ценой для передачи трафика.

На устройство CPE заранее загружаются правила использования резервного WAN-порта, если путь через основной WAN-порт становится недоступным. В этом случае при нарушении работы основного наложенного туннеля не производится переписывание правил коммутации пакетов, и устройство CPE отправляет их через резервный порт.

Вы можете настроить резервирование на уровне сервисов. В этом случае при создании транспортного сервиса для одного или всех сервисных интерфейсов можно указать резервный сервисный интерфейс (англ. reserve SI) на выбранном устройстве CPE или на другом устройстве. Решение поддерживает создание резервных сервисных интерфейсов для всех типов транспортных сервисов уровня L2.

Трафик переключается на резервный сервисный интерфейс, если основной сервисный интерфейс недоступен. Мы рекомендуем создавать основной и резервный сервисные интерфейсы на разных устройствах. Например, вы можете применить эту функцию для резервирования шлюзов SD-WAN. В этом случае при создании транспортного сервиса в качестве основного сервисного интерфейса вам нужно указать порт на первом шлюзе SD-WAN и в качестве резервного сервисного интерфейса указать порт на втором шлюзе SD-WAN. Для создания транспортного сервиса вам нужно перейти в раздел **Инфраструктура** ( ) веб-интерфейса оркестратора, открыть страницу настройки контроллера или узла контроллера SD-WAN, после чего перейти в раздел требуемого транспортного сервиса, например в раздел **P2P сервисы**.

На рисунке ниже приведен пример сервиса SD-WAN с двумя шлюзами и тремя устройствами CPE. Каждое устройство CPE использует по два WAN-порта. Первый шлюз SD-WAN является основным, в то время как

второй выполняет функцию резервного. Устройства CPE прокладывают по одному наложенному туннелю до каждого шлюза SD-WAN через все WAN-порты.

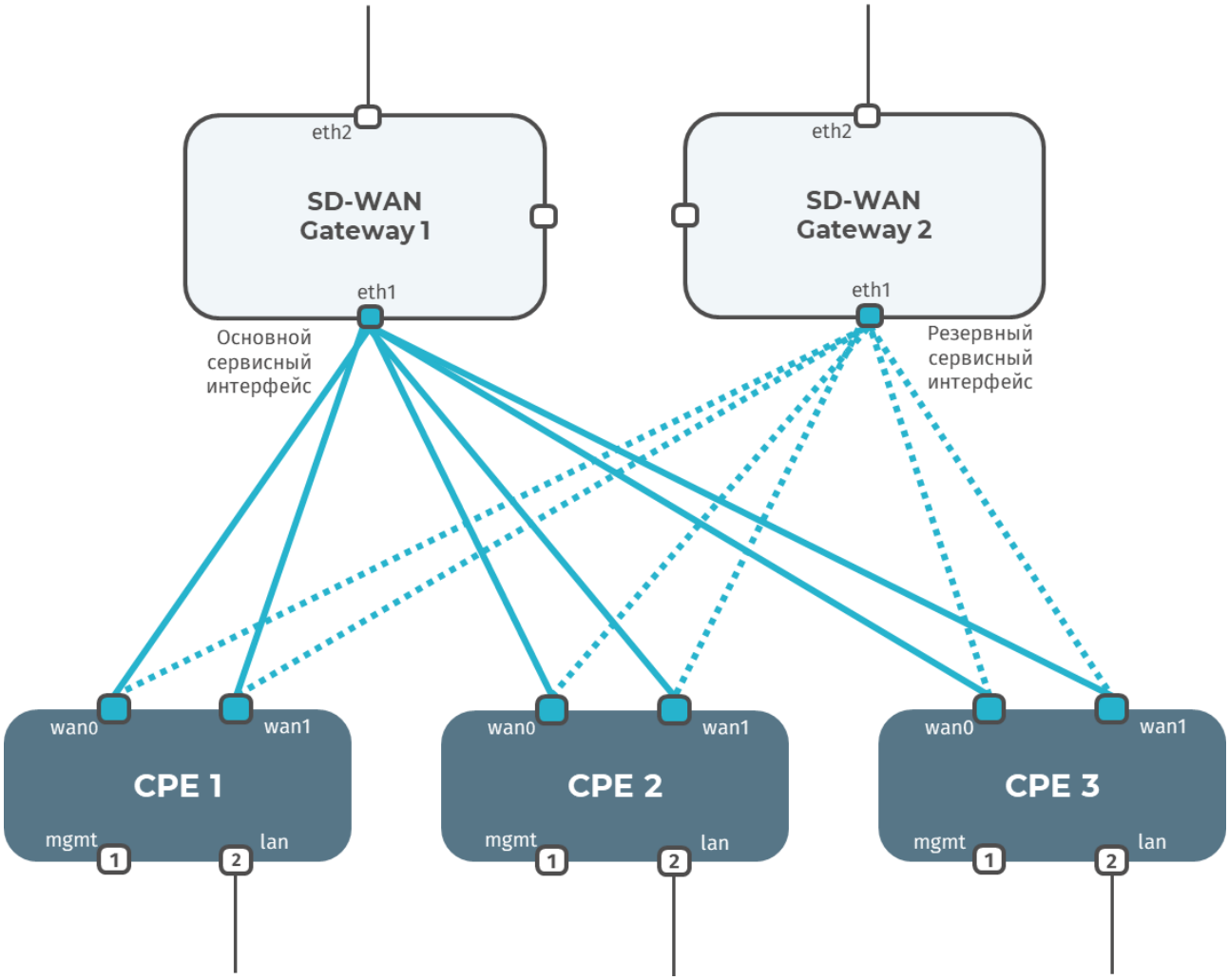

Рисунок 14. Сервис SD-WAN, использующий резервирование

Контроллер SD-WAN можно развернуть как один узел или кластер из трех узлов. Пользовательский трафик не проходит через контроллер SD-WAN, поэтому если контроллер SD-WAN недоступен, то передача трафика между устройствами CPE и шлюзами SD-WAN не прекращается.

О функции Dampening

Функция Dampening – это настраиваемый механизм, который ограничивает доступ к нестабильным сервисным интерфейсам, состояние которых меняется слишком часто. Нестабильные сервисные интерфейсы потребляют большое количество сетевых ресурсов и затрудняют передачу трафика по транспортным путям.

Вы можете использовать функцию Dampening, чтобы выполнять следующие задачи:

- обнаруживать частые изменения состояния сервисных интерфейсов, например изменение статуса UP-DOWN;
- перемещать сервисы, проходящие через сервисные интерфейсы на запасные транспортные пути;

- исключать транспортные сегменты, привязанные к сервисным интерфейсам из расчета транспортных путей для сервисов.

Для включения функции Dampening вам нужно перейти в раздел **Инфраструктура** ( ) веб-интерфейса оркестратора, открыть страницу настройки контроллера или узла контроллера SD-WAN, после чего перейти в раздел **Линки**. В этом разделе вам потребуется выбрать виртуальный канал, чтобы включить на нем функцию Dampening. Вы можете изменить параметры функции Dampening (см. таблицу ниже), если вам не подходят значения, указанные по умолчанию.

Таблица 16. Описание параметров функции Dampening

Параметр	Описание
Максимально допустимое время блокировки (мсек)	Максимальное время в миллисекундах, в течение которого доступ к сервисному интерфейсу может быть ограничен. По истечении этого времени все счетчики на сервисном интерфейсе сбрасываются.
Штраф	Число, которое будет добавляться к показателю Penalty сервисного интерфейса при изменении состояния этого сервисного интерфейса.
Порог блокировки	Значение показателя Penalty, при котором доступ к сервисному интерфейсу будет ограничен.
Интервал обновления (мсек)	Время в миллисекундах, в течение которого показатель Penalty сервисного интерфейса должен будет набрать значение, указанное в поле **Порог блокировки**, чтобы доступ к этому сервисному интерфейсу был ограничен.

По умолчанию сервисный интерфейс и связанный с ним транспортный сегмент начинают работать, если состояние этого сервисного интерфейса не меняется в течение 10 минут.

kaspersky

Обеспечение безопасности

В этом разделе содержится информация о том, как в рамках решения Kaspersky SD-WAN обеспечивается безопасность сетей SD-WAN.

Безопасность в рамках решения Kaspersky SD-WAN обеспечивается на уровнях передачи данных, управления сетью и оркестрации. Безопасность всего решения определяется безопасностью каждого из этих уровней, а также безопасностью их сообщения. Для обеспечения безопасности на каждом уровне происходят следующие процессы:

- 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 Kaspersky SD-WAN также поддерживает безопасное подключение устройств CPE.

В этом разделе

Аутентификация и авторизация пользователей

Управление решением осуществляется с помощью веб-интерфейса оркестратора или с помощью API. Устройства CPE также могут обладать графическими интерфейсами. Остальные компоненты решения не имеют графического интерфейса. Чтобы получить доступ к управлению решением через веб-интерфейс оркестратора или с помощью API, пользователю нужно авторизоваться.

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, которую вы добавляете с помощью сервера LDAP и, если требуется, привязывает их к тенанту.

Учетные записи локальных пользователей создаются в графическом веб-интерфейсе оркестратора на вкладке **Пользователи**. После того, как вы создаете учетную запись, она является неактивной. Вам нужно активировать учетную запись, чтобы пользователь смог войти в систему.

Использование безопасных протоколов управления

Мы рекомендуем использовать протокол HTTPS при взаимодействии с сервисом SD-WAN через веб-интерфейс оркестратора или с помощью API. Вы можете использовать собственные сертификаты, которые

требуется заранее загрузить в систему, или автоматически сгенерированные самоподписанные сертификаты. Решение Kaspersky SD-WAN использует несколько протоколов для передачи управляющего трафика компонентам сервиса SD-WAN (см. таблицу ниже).

Таблица 17. 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	Нет значения.
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:

- Идентификация устройства CPE с помощью идентификатора DPID.
- Отложенная регистрация.

  Вы можете выбрать, в каком состоянии будет находиться устройство CPE после успешной регистрации – во включенном или выключенном. Выключенное устройство CPE требуется включить вручную, убедившись, что оно установлено на нужной площадке.
- Двухфакторная активация.

  Клиент получает ключ, который требуется ввести на устройстве CPE для его активации.

В ходе регистрации устройство CPE отправляет оркестратору свой идентификатор DPID. Оркестратор ищет идентификатор DPID, полученный от устройства CPE в инвентаризационной базе. Если этот идентификатор DPID существует, то оркестратор передает устройству CPE информацию, необходимую для подключения к сети. Если переданный идентификатор DPID отсутствует в инвентаризационной базе, то устройство отображается в списке устройств CPE со статусом *Неизвестно* и не подключается к сети SD-WAN.

После активации устройства CPE и его подключения к сервису управления SD-WAN managementTunnel компонент VNFM загружает на него нужную конфигурацию. Вы можете разрешить или запретить локальное изменение загруженной конфигурации устройства CPE. Перед удалением устройства CPE вы можете очистить его конфигурацию.

kaspersky

О защите данных с помощью VNF

Вы можете обеспечить дополнительный уровень безопасности с помощью VNF, развернутых в ЦОД поставщика услуг. Например, трафик может быть направлен от устройства CPE к VNF, которая выполняет функцию сетевого экрана или прокси-сервера. Вы можете запустить VNF непосредственно на устройстве CPE, если оно обладает достаточными аппаратными ресурсами.

Например, VNF могут выполнять следующие функции защиты сети SD-WAN:

- межсетевой экран нового поколения (англ. Next-Generation Firewall, NGFW);
- защита от атак DDoS (Distributed Deinal 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.

Топологии сетей SD-WAN

В этом разделе содержится информация о топологиях, которые вы можете использовать при построении сетей SD-WAN с помощью решения Kaspersky SD-WAN. Топология сети SD-WAN определяется транспортными сервисами, которые вы выбираете в шаблоне экземпляра SD-WAN.

В этом разделе

О топологии Hub-and-Spoke без связи между удаленными офисами

Топология Hub-and-Spoke является наиболее распространенной при построении сетей SD-WAN. В этом разделе описывается топология Hub-and-Spoke, в рамках которой удаленные площадки подключаются к центральному офису и не могут напрямую связываться друг с другом (см. рисунок ниже). Сети SD-WAN, построенные с применением такой топологии просты в проектировании и обслуживании, потому что все необходимые сервисы и приложения размещаются в центральном ЦОД.

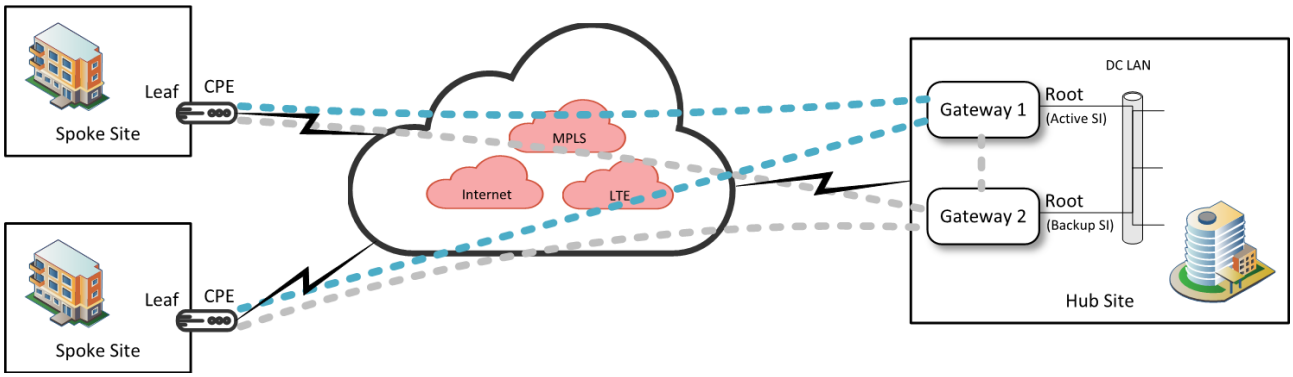

Рисунок 15. Топология Hub-and-Spoke без связи между удаленными офисами

Чтобы построить топологию Hub-and-Spoke без связи между удаленными офисами, вам нужно создать транспортный сервис L2 типа P2M (Point-to-Multipoint или E-tree) в шаблоне экземпляра SD-WAN.

Для настройки шаблона экземпляра SD-WAN вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора, после чего перейти в подраздел **SD-WAN шаблоны экземпляров** ( ).

В качестве конечных сервисных интерфейсов требуется указать порты на шлюзах SD-WAN 1 и 2. Этим сервисным интерфейсам будет назначена роль Root. Устройства CPE, регистрирующиеся в оркестраторе, автоматически включаются в транспортный сервис с ролью Leaf. Вы можете применить механизмы NAT (Network Address Translation) и PAT (Port Address Translation) к устройствам CPE.

В рамках этой топологии Hub-and-Spoke запрещается передача трафика напрямую между устройствами CPE, а также через шлюзы SD-WAN. Вы можете использовать параметры QoS (Quality of Service), чтобы ограничить полосу пропускания для устройств CPE или определенных классов трафика.

См. также

О шаблоне экземпляра SD-WAN.....19

О топологии Hub-and-Spoke со связью между удаленными офисами через центральный офис

В этом разделе описывается топология Hub-and-Spoke, в рамках которой все офисы могут связываться друг с другом через центральный офис (англ. hub) (см. рисунок ниже).

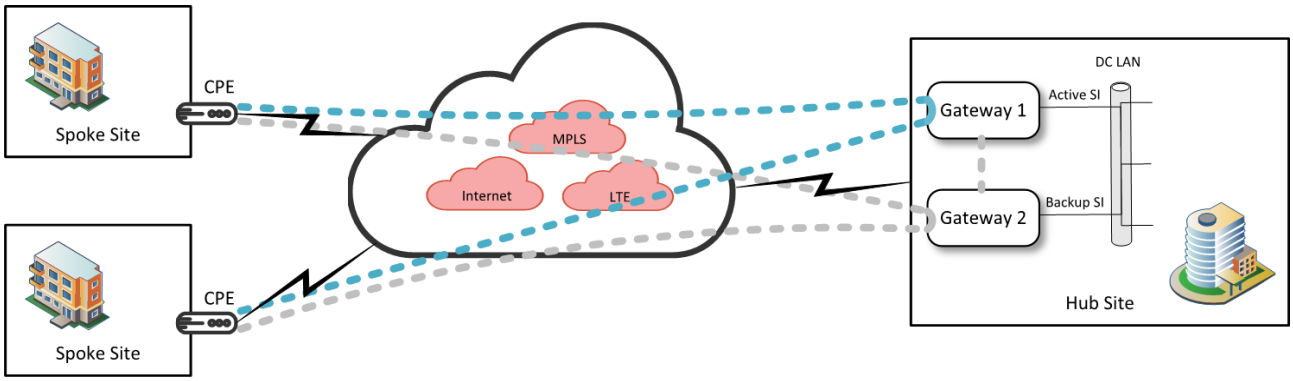

Рисунок 16. Топология Hub-and-Spoke со связью между удаленными офисами

Чтобы построить топологию Hub-and-Spoke со связью между удаленными офисами через центральный офис, вам нужно создать транспортный сервис L2 типа M2M (Multipoint-to-Multipoint или E-LAN) в шаблоне экземпляра SD-WAN. Для настройки шаблона экземпляра SD-WAN вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора, после чего перейти в подраздел **SD-WAN шаблоны экземпляров** ( ).

В качестве конечных сервисных интерфейсов требуется указать порты на шлюзах SD-WAN 1 и 2. Устройства CPE, регистрирующиеся в оркестраторе, автоматически включаются в транспортный сервис. Вы можете применить механизмы NAT и PAT к устройствам CPE.

Вы можете использовать параметры QoS (Quality of Service), чтобы ограничить полосу пропускания для устройств CPE или определенных классов трафика.

См. также

О шаблоне экземпляра SD-WAN.....19

О топологии Hub-and-Spoke со связью между офисами через сервисную цепочку в ЦОД

В этом разделе описывается топология Hub-and-Spoke, в рамках которой трафик между площадками проходит через VNF, развернутые в ЦОД (см. рисунок ниже). Это позволяет выполнять такие задачи, как обеспечение безопасности межсетевого обмена, наблюдение за пакетами и кеширование данных.

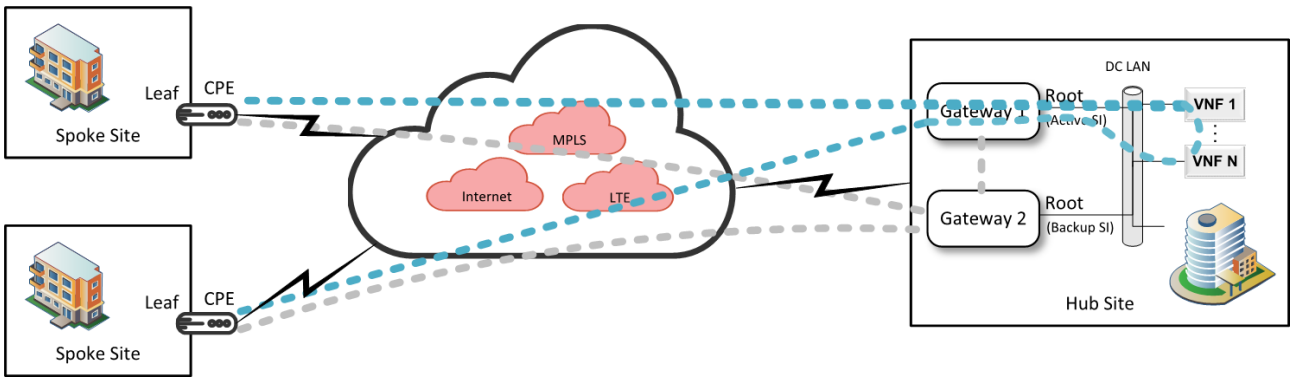

Рисунок 17. Топология Hub-and-Spoke со связью между офисами через сервисную цепочку

Чтобы построить топологию Hub-and-Spoke со связью между офисами через сервисную цепочку в ЦОД, вам нужно создать транспортный сервис L2 типа P2M (Point-to-Multipoint или E-Tree) в шаблоне экземпляра SD-WAN. Для настройки шаблона экземпляра SD-WAN вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора, после чего перейти в подраздел **SD-WAN шаблоны экземпляров** ( ). Вам также нужно убедиться, что сетевой сервис SD-WAN, развернутый для тенанта, содержит в цепочке все требуемые VNF.

См. также

О шаблоне экземпляра SD-WAN.....19

О настройке сервиса L3 VPN

Вы можете использовать сервис L3 VPN со статической маршрутизацией для создания маршрутизируемой сети между сетями клиента с возможностью добавления статических маршрутов. Если вам нужно использовать динамическую маршрутизацию, то вы можете создать транспортный сервис L2 P2M в шаблоне экземпляра SD-WAN, затем включить в сервисную цепочку VNF, выполняющую функцию маршрутизатора. Для настройки шаблона экземпляра SD-WAN вам нужно перейти в раздел **SD-WAN** ( ) веб-интерфейса оркестратора, после чего перейти в подраздел **SD-WAN шаблоны экземпляров** ( ).

См. также

О шаблоне экземпляра SD-WAN.....19