Kaspersky SD-WAN

Руководство по настройке демонстрационного стенда Kaspersky SD-WAN в среде VMware

Часть 2

Настройка сценариев классификации, приоритезации и управления трафиком, построения Full-Mesh и Partial-Mesh топологий, обновление CPE устройств, резервирование CPE с помощью VRRP.

Содержание

1. Kaspersky SD-WAN.	3
1.1. Архитектура решения Kaspersky SD-WAN	4
2. Описание схемы демонстрационного стенда Kaspersky SD-WAN	5
2.1. Схема демонстрационного стенда	6
2.2. Сетевые порты, используемые центральными компонентами решения	7
2.3. План IP адресации	8
2.4. Версии программного обеспечения.	10
2.5. Требования к аппаратным ресурсам решения Kaspersky SD-WAN	10
3. Управление трафиком	11
3.1. Балансировка нагрузки в режиме Active / Active	12
3.2. Резервирование каналов связи в режиме Active/Standby	20
3.3. Резервирование каналов связи в широковещательном (broadcast) режиме	27
3.4. Повышение надежности каналов с использованием механизма Forward Error Correction (FEC)	32
3.5. Мониторинг качества туннелей (Jitter, Latency, Packet Loss) и управление трафиком в соответствии с заданным SLA	40
3.6. Приоритезация трафика с использованием ACL	50
3.7. Приоритезация трафика с использованием DPI	61
4. Построение топологии SD-WAN сети	72
4.1. Создание топологий Full-Mesh	73
4.2. Создание топологий Partial-Mesh	76
4.3. Создание топологий с использованием транзитных СРЕ	80
5. Работа с СРЕ устройствами	83
5.1. Централизованное обновление firmware CPE устройств	83
5.2. Резервирование устройств СРЕ с использованием VRRP	88
Приложение А.	96
Checklist	96

1. Kaspersky SD-WAN.

Решение Kaspersky SD-WAN используется для построения программно-определяемых распределенных сетей (англ. Software Defined WAN или SD-WAN) для маршрутизации сетевого 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, или 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. Данный контроллер взаимодействует с устройствами CPE, составляющими уровень передачи данных, а также с SD-WAN оркестратором, который используется для управления сетью SD-WAN с помощью веб-интерфейса.

Решение Kaspersky SD-WAN предназначено для операторов связи, компаний, имеющих крупную филиальную сеть, и используется для замены стандартных маршрутизаторов в распределенных сетях.

Решение Kaspersky SD-WAN обладает следующими основными характеристиками:

- Работа на основе проводных и беспроводных сетей любого типа.
- Использование несколько виртуальных каналов для обеспечения высокой доступности сети и балансировки трафика.
- Коррекция ошибок при передаче данных.
- Интеллектуальное управление трафиком.
- Автоматическая настройка устройств СРЕ с использованием концепции Zero Trust Provisioning (ZTP).
- Централизованное управление и мониторинг.

1.1. Архитектура решения Kaspersky SD-WAN.

Краткое описание основных компонентов решения Kaspersky SD-WAN:

- SD-WAN оркестратор. Предоставляет единый графический веб-интерфейс управления, отвечает за управление сервисами SD-WAN сети и содержит инвентаризационную базу СРЕ устройств.
- SD-WAN контроллер. Управляет наложенной сетью (англ. Overlay Network), обеспечивает построение топологии сети и создание транспортных сервисов внутри наложенных туннелей. Поддерживает транспортные сервисы L2 Point-to-Point (P2P), Point-to-Multipoint (P2M), Multipoint-to-Multipoint (M2M) и L3 VPN. Управляет устройствами СРЕ и шлюзами SD-WAN по протоколу OpenFlow. Определяет распределение трафика между туннелями, выполняет мониторинг качества соединения и автоматическое переключение трафика на резервный туннель в случае возникновения проблем на основном. Контроллер находится под управлением SD-WAN оркестратора.
- SD-WAN шлюзы. Объединяют СРЕ устройства в единую сеть. Наложенные туннели терминируются на SD-WAN шлюзах, после чего трафик передается дальше в соответствии с топологией сети.
- СРЕ устройства или Kaspersky Edge Service Router (KESR). Телекоммуникационное оборудование, которое подключается к шлюзам SD-WAN с помощью наложенных туннелей и образует SDN-фабрику в виде наложенной сети.

Архитектура решения Kaspersky SD-WAN представлена на рисунке 1.



Рисунок 1. Архитектура решения Kaspersky SD-WAN.

2. Описание схемы демонстрационного стенда Kaspersky SD-WAN.

Все компоненты демонстрационного стенда Kaspersky SD-WAN развернуты в среде виртуализации VMware.

Развертывание и базовая настройка демонстрационного стенда описаны в первой части документа Proof of Concept Руководство по настройке демонстрационного стенда Kaspersky SD-WAN Часть 1.

На виртуальном хосте orc1 развернуты Docker контейнеры решения Kaspersky SD-WAN, включая оркестратор, контролер и систему мониторинга Zabbix.

Логическая схема демонстрационного стенда Kaspersky SD-WAN представлена на рисунке 2. Демонстрационный стенд включает в себя:

- Площадка DC с сетевыми сегментами dc-lan1 и oob, подключенными к маршрутизатору R13. Виртуальная машина SD-WAN оркестратора orc1 размещена в сегменте oob, сервер srv1 с WWW службой размещен в сегменте dc-lan1.
- На границе DC размещены два маршрутизатора R11 и R12, за которыми размещены два SD-WAN шлюза: vGW-11 и vGW-12. Внутренние (lan) интерфейсы R13, vGW-11 и vGW-12 подключены к сетевому сегменту dc-perim.
- Маршрутизаторы R11 и R12 выполняют функцию SNAT для vGW-11 и vGW-12 и DNAT для портов, указанных в Таблице №1.
- Маршрутизатор R14 выполняет SNAT, роль шлюза по умолчанию для R13, и выход в Интернет для хоста orc1. R14 выполняет DNAT для хоста orc1 для портов, указанных в Таблице №1 для Docker контейнеров SD-WAN оркестратора и SD-WAN контроллера.
- Хост ISP эмулирует подключение к сети Интернет / операторам связи ISP1 ISP8.
- Для подключения CPE устройств SD-WAN шлюзы должны быть доступны по определённому набору портов, перечисленных в Таблице №1.
- Устройство vCPE-3 представляет собой пример подключения удаленной площадки с одним CPE устройством, подключенным к двум операторам связи.
- Устройство vCPE-4 представляет собой пример будущего, не рассматриваемой в рамках текущего стенда, подключения удаленной площадки с универсальным uCPE устройством.
- Шлюзы vCPE-51 и vCPE-52 представляют собой пример подключения удаленной площадки с двумя CPE устройствами. Для отказоустойчивости используется протокол VRRP.

2.1. Схема демонстрационного стенда.

Схема демонстрационного стенда Kaspersky SD-WAN представлена на рисунке 2.



Рисунок 2 – Демонстрационный стенд Kaspersky SD-WAN 2.0

2.2. Сетевые порты, используемые центральными компонентами решения.

Компонент	Порт	Назначение
SD-WAN оркестратор	TCP 82 TCP 85	Доступ к веб- интерфейсу СРЕ через веб- интерфейс оркестратора.
	TCP 443	Доступ к веб- интерфейсу Zabbix. Доступ к веб- интерфейсу оркестратора.
SD-WAN контроллер	TCP 6653-6656	Подключение SD-WAN шлюзов и CPE устройств к контроллеру по TLS. CPE устройство подключается каждым wan интерфейсом к отдельному порту контроллера: • sdwan0 - 6653 • sdwan1 - 6654 • и т.д.
SD-WAN шлюзы	UDP 4800	Дата трафик.

Таблица 1. – Сетевые порты для взаимодействия SD-WAN шлюзов и СРЕ устройств с центральными компонентами решения, и доступ к веб- интерфейсу оркестратора для администрирования решения.

2.3. План ІР адресации.

Данный IP план соответствует схеме из пункта 2.1 в случае использования других адресов требуется изменить план и все настройки SD-WAN в дальнейших шагах.

Имя	Операционная	IP адрес	Назначение	Минимальные
	система			ресурсы
orc1	Ubuntu	10.0.1.11	На хосте	24 x vCPU, 32 GB
	20.04.06 LTS		развернуты	RAM
	Server		Docker	
			контейнеры:	
			www-1, orc-1,	
			redis-1m, mongo-	
			1, vnfm-1, vnfm-	
			proxy-1, ctl,	
			zabbix-www-1,	
			zabbix-srv-1,	
			zabbix-prx-1,	
			zabbix-db-1,	
			syslog-1	
vGW-11	CPEOS	wan 10.1.4.11	SD-WAN шлюз	4 x vCPU, 2 GB
		lan 10.1.3.11		RAM
vGW-12	CPEOS	wan 10.1.5.12	SD-WAN шлюз	4 x vCPU, 2 GB
		lan 10.1.3.12		RAM
vCPE-3	CPEOS	wan DHCP	CPE	4 x vCPU, 2 GB
		lan 10.20.3.1		RAM
vCPE-4	CPEOS	wan DHCP	CPE	4 x vCPU, 2 GB
		lan 10.20.4.1		RAM
vCPE-51	CPEOS	wan DHCP	CPE	4 x vCPU, 2 GB
		lan 10.20.5.1		RAM
vCPE-52	CPEOS	wan DHCP	CPE	4 x vCPU, 2 GB
		lan 10.20.5.2		RAM
R11	CentOS 7	wan 10.50.1.11	Пограничный	2 x vCPU, 2 GB
		lan 10.1.4.1	маршрутизатор	RAM
			DC	
R12	CentOS 7	wan 10.50.2.12	Пограничный	2 x vCPU, 2 GB
		lan 10.1.5.1	маршрутизатор	RAM
			DC	
R13	CentOS 7	dc-perim 10.1.3.13	Маршрутизатор	2 x vCPU, 2 GB
		oob 10.0.1.13	ядра DC	RAM
		dc-lan1 10.1.1.1		

Имя	Операционная система	IP адрес	Назначение	Минимальные ресурсы
R14	CentOS 7	wan 10.50.1.14 lan 10.1.3.1	Пограничный маршрутизатор DC, NAT	2 x vCPU, 2 GB RAM
ISP	CentOS 7	isp1 10.50.1.1 isp2 10.50.2.1 isp5 10.50.5.1 isp6 10.50.6.1 isp7 10.50.7.1 isp8 10.50.8.1	Эмуляция ISP1— ISP8	2 x vCPU, 2 GB RAM
srv1	CentOS 7	10.1.1.11	Сервер WWW/DC	2 x vCPU, 4 GB RAM
wst3	CentOS 7	10.20.3.11	Рабочая станция Site3	2 x vCPU, 4 GB RAM
wst4	CentOS 7	10.20.4.11	Рабочая станция Site4	2 x vCPU, 4 GB RAM
wst5	CentOS 7	10.20.5.11	Рабочая станция Site5	2 x vCPU, 4 GB RAM
mgmt	Windows 11	10.0.1.10 10.1.1.10 10.1.3.10 10.50.1.10 10.20.3.10 10.20.4.10 10.20.5.10	Рабочая станция для управления демо стендом.	6 x vCPU, 6 GB RAM

2.4. Версии программного обеспечения.

Таблица №3 – Версии программного обеспечения Kaspersky SD-WAN, используемого в данном демонстрационном стенде:

Компонент SD-WAN	Версия
www	knaas-www:2.23.07.release.81.amd64_en-US_ru-RU
orc	knaas-orc:2.23.07.release.88.amd64_en-US_ru-RU
mongo	mongo:5.0.7.amd64
ctl	knaas-ctl:2.23.07.release.39.amd64_en-US_ru-RU
vnfm	knaas-vnfm:2.23.07.release.8.amd64_en-US_ru-RU
vnfm-proxy	knaas-vnfm-proxy:2.23.07.release.2.amd64_en-US_ru-RU
redis	redis:6.2.7.amd64
zabbix-www	zabbix-web-nginx-mysql:5.0.32.amd64
zabbix-proxy	zabbix-proxyr-mysql:5.0.32.amd64
zabbix-srv	zabbix-server-mysql:5.0.32.amd64
zabbix-db	mariadb:10.4.28.amd64
syslog	syslog-ng:3.30.1.amd64
VCPE	knaas-cpe_2.23.07.release.23.combined.amd64-legacy.qcow2
Xoct orc1	Ubuntu 20.04.06 LTS Server
installer	knaas-installer_2.23.07.release.29.amd64_en-US_ru-RU.tar.gz

2.5. Требования к аппаратным ресурсам решения Kaspersky SD-WAN.

Таблица №4 - Требования к аппаратным ресурсам для управления до 50 СРЕ устройств.

Хост	CPU (hyper-	RAM, GB	Disk, GB, SSD
	threading), cores		Используется в данной
			конфигурации /
			Рекомендуется
orc1	24	32	50 / 265

3. Управление трафиком.

Соединение между устройствами СРЕ устанавливается через туннели GENEVE, которые строятся поверх каналов передачи данных. Туннели (линки) являются однонаправленными, поэтому при соединении двух устройств СРЕ требуется входящий и исходящий туннель.

Совокупность туннелей, соединяющих два устройства СРЕ, является сегментом. Трафик может быть распределен по нескольким туннелям на устройстве СРЕ- отправителе в начале сегмента и передан устройству СРЕ- получателю в конце сегмента.

Маршруты, по которым трафик может быть передан в рамках одного сегмента, являются транспортными путями. Поддерживается использование следующих типов транспортных путей:

- Auto-SPF (Shortest-Path Forwarding). Автоматически рассчитываемый контроллером SD-WAN транспортный путь. Транспортные пути этого типа невозможно добавлять и удалять, а также изменять их параметры.
- Manual-TE (Traffic Engineering). Транспортный путь, который добавляется вручную. Для добавления транспортного пути этого типа требуется указать параметры туннелей, через которые транспортный путь будет проходить от устройства СРЕ в начале сегмента до устройства СРЕ в конце сегмента.
- Auto-TE. Автоматически рассчитываемый контроллером SD-WAN транспортный путь, учитывающий преднастроенные ограничения (англ. constraints). Ограничениями могут быть значения показателей мониторинга на туннелях, например, показатель уровня загрузки туннеля.

Транспортные пути имеют следующие параметры:

- Стоимость (англ. Path.cost). По умолчанию, является суммой стоимости всех туннелей, которые входят в транспортный путь. Поддерживается возможность ручного определения стоимости транспортных путей.
- Вес (англ. Path.weight).
- Административное состояние (англ. Path.admin.state). Задается вручную. Если этот параметр имеет значение down, транспортный путь не используется.
- Фактическое состояние (англ. Path.oper.state). Зависит от наличия или отсутствия возможности передачи трафика. Если этот параметр имеет значение down, транспортный путь не используется.

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

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help > Туннели, сегменты и транспортные пути: <u>https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/250984.htm</u>

3.1. Балансировка нагрузки в режиме Active / Active.

Kaspersky SD-WAN обеспечивает защиту от перерывов связи с устройствами CPE с помощью одновременного использования всех доступных каналов передачи данных. Поддерживаются следующие режимы резервирования каналов передачи данных: Active/Active и Active/Standby.

Для получения дополнительной информации о резервировании каналов связи обратитесь к Kaspersky SD-WAN Online Help > Резервирование каналов передачи данных между устройствами CPE: <u>https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/239053.htm</u>

В данном сценарии рассматривается сценарий балансировки нагрузки между интерфейсами устройства vCPE-3. На устройстве vCPE-3 используется пара WAN интерфейсов в режиме Active / Active. Для балансировки нагрузки используется параметр Cost туннелей.

Для демонстрации балансировки трафика между vCPE-3 и vCPE-4 на рабочих станциях wst3 и wst4 используется генератор трафика iperf. Для проверки работы балансировки будет использована встроенная система мониторинга.

3.1.1. Просмотр построенных сегментов SD-WAN фабрики.

Для отображения перечня всех сегментов SD-WAN фабрики перейти в меню Infrastructure > SD-WAN Cluster > Management > Open configuration menu > Segments.

	astructure × + C A Not secure https://10.0.1.1	/infrastructure?controllerID=6527d46b8981ea44fcb	b69584&mode=network				v – t Q છે ✿ □
	Infrastructure				+ Domain +	Data center + VIM	+ Controller + Sub
୬ ଅ େ ାା = େ ୦ ୫ ସା େ ≪	Q All <u>Domain</u> <u>Data center</u> All resources * <u>demolab space</u> ₽ <u>DC</u>	Network resources Compute resources System Name - I Trans I SD-WAN Cluster (tenant: 6527d10/898iee44fcb69576) Genet grans	resources IPAM iport/service strategy 1 ric VNI swapping port	Controller nodes 10.111.97 (primary)	: Connection type Unicast	Cluster status Node statuses DEGRADED Connected (sing)	e) Management EGIT Open configuration menu Reprovision Download backup file Restore Delete Open properties
На чет СР	скриншоте пр гырех транспој È с ролью Gat	едставлен пример отных путей (path) eway: vGW-11 и v(о сегмент) типа Au GW-12.	га между v to SPF. Тр	′СРЕ-4 и ∨ ранспортнь	СРЕ-3, состоя ые пути прохо,	іщий из дят через



egments	e.	×	+									~			1
C	A Not secur	e hi	tps://10.0.1.11	1/controller/segr	ment?controllerID	=640978ef84	7e04a332d5c2e					2 10 4	*		1
	Segments														
	From	i T	īo i	Path count / Max	Path number	Path type	Paths	Admin state	Oper state	Cost	Hop count		0	Q	1
												ĉ		1	
	CPE [vCPE 4:	- 0	SPE [VCPE-	4/8	0	Auto SPF	CPE [vCPE-4: 80000050568E7383] : 4800 → CPE [vGW-12: 80000050568EC85F] : 4800 CPE [vGW-12: 80000050568EC85F] : 4800 → CPE [vCPE-3: 80000050568EEDAE] : 4800	up	up	20000	2	Manage	ment		
	8000005	056 8	3000005056	6	1	Auto SPF	CPE [vCPE-4: 80000050568E7383] : 4801 → CPE [vGW-12: 80000050568EC85F] : 4800 CPE [vGW-12: 80000050568EC85F] : 4800 → CPE [vCPE-3: 80000050568EEDAE] : 4801	up	up	20000	2				
					2	Auto SPF	CPE [vCPE-4: 80000050568E7383] : 4800 → CPE [vGW-11: 80000050568EDB3F] : 4800 CPE [vGW-11: 80000050568EDB3F] : 4800 → CPE [vCPE-3: 80000050568EEDAE] : 4800	up	up	20000	2				
					3	Auto SPF	CPE fvCPE-4: 80000050568E73831: 4801 → CPE fvGW-11: 80000050568EDB3F1: 4800	UD	UD	20000	2				

Стоимость (Cost) каждого из четырех путей равна, значение 20000, поэтому трафик равномерно балансируется между всеми транспортными путями в рамках сегмента между vCPE-4 и vCPE-3.

Балансировка осуществляется средствами протокола OpenFlow (группы типа Select).

Для получения дополнительной информации о параметрах балансировки нажать кнопку Management > Edit.

/laximum numbei 8	r of paths ၇		Ma 4	aximun L	n number of A	uto-SPF paths ⊘	Cost var	riance multiplier 곗	
nable multi weig	ht 🕐								
ransport paths	Administr	rative	Operatio	nal					
# Type	state		state		Cost	Hop count	Load bala	ancing	-1
) Auto SPF	Up	~	Yes	~	20000	2	Up	~	
Auto SPF	Up	~	Yes	~	20000	2	Up	~	- 1
2 Auto SPF	Up	~	Yes	~	20000	2	Up	~	
3 Auto SPF	Up	~	Yes	~	20000	2	Up	~	
						J			

Контроллер заранее просчитывает все возможные транспортные пути, в том числе и резервные, например, если, фактическое количество транспортных путей больше, чем задано в параметре Maximum number of Auto-SPF paths для конкретного сегмента. Как только будет обнаружено событие отказа туннеля (линка) между CPE устройствами, туннель будет удален из топологии, а трафик перенаправлен на резервный транспортный путь.

3.1.2. Выбор режима балансировки.

Доступные режимы балансировки:

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

To configure the balancing mode, go to **Infrastructure > SD-WAN Controller > Management > Open configuration menu**.

Infra:	structure × +		v – 6
$\leftarrow \ \rightarrow$	C A Not secure https://10.0.1.1	1/infrastructure?controllerID=6527d46b8981ea44fcb69584&mode=network	역 년 🖈 🛛
	Infrastructure		+ Domain + Data center + VIM + Controller + Sub-
»	Resources Q	Network resources Compute resources System resources IPAM	
	All Domain Data center	Name	Connection type : Cluster status : Node statuses :
5	All resources	SD-WAN Cluster [tenant: Generic VNI swapping 10.11.11.97 (primary) 6527d10f9981ea44fcb69576] transport	Unicast DEGRADED Connected (single) Management
o	* demolab.space		Edit
Ň	早 <u>DC</u>		Open configuration menu
ŭ			Reprovision
			Download backup file
:=			Restore
0			Delete
ő			Open properties
er			

Go to the section with M2M transport services. Select the transport service to edit, click **Management > Edit**.

Kaspersky SD-WAN M2M Services							+ Create a new M2M service
>>> Back to Main Menu	X ALI	UP DOWN DEGRA	DED				
Controller Nodes Switches	: MAC age timeout	MAC address learn mode	MAC table size	MAC table overload action	Endpoints	: : Status Description	: @
Topology	300	Learn and Flood	100	Flood	SI://CPE [vGW-11: 8000005056AA9EA5]/p:2	UP	Management
Segments					SI://CPE [vGW-12: 80000050566AAD2B1]/p:2		
QoS					SI://CPE [vCPE-3: 8000005056AAC4FD]/p:2		
P2P Services					SI://CPE [vCPE-4: 8000005056AA35FF]/p:2		
M2M Services					8000005056AAB512]/p.2 SI://CPE [vCPE-52:		
IP Multicast Sources					8000005056AAC6B5]/p.2		
L3 Static VPN							
TAP							
Service Interfaces							
Constraints							
Filter							



3.1.3. Включение режим балансировки Per-packet.

Для теста требуется включить режим балансировки Per-packet в связи с тем, что в сценарии для генерации трафика используется iperf, работающий по одному порту. При использовании режима балансировки Per-flow будет задействован только один WAN интерфейс CPE-устройства.

Выбрать Balancing Mode – Per-packet.

	M2M Services				+ Create a new M2M service
>>		Edit M2M Service	>	<	
-					
Con	1.110	Name			:
Swit	Name MAC age timeout	L2 M2M		Description	¢
-		Constraint	Balancing Mode		
Iop	L2 M2M 300	Threshold 🗸	Per-packet 🗸		Management
Тор		MAC address loss	MACtoble		
Seg		mode MAC age timeout	overload action MAC table size		
QoS		Learn and Flo 🗸 300	Flood v 100		
P2P		Description			
P2N					
M21			h		
IP M					
L3 S		Cancel	Next		
TAP					
EN	© 2023 AO "Kaspersky Lab" support.k	aspersky.com	Version: 2.23.03.release.94.amd6	4-SNAPSHOT / 2.2	3.03.release.93.amd64-SNAPSHOT

Нажать Next, Next и Save.

Для получения справочной информации о режимах балансировки обратитесь к Kaspersky SD-WAN Online Help > Создание M2M-сервиса: <u>https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/245696.htm</u>

3.1.4. Просмотр построенных туннелей СРЕ.

Перейти в меню СРЕ и выбрать vCPE-3.

>>	ODE													C	Exp
<u>ш</u>		c Waiting c Cor	figuration	Registered o	Registering	• Error	- Unknown	All tin	ne Lastyear	Last month	Last week	Last day 14/11/2	023 10:41 - 1	4/11/2023 10:41	
¢.	All 6	DPID :	Model :	SW version	Name :	Role :	Status :	State	Connection :	Fragmentation	Usage :	Transport tenant :	Customer tenant :	Registered 🛞 C	ر. Acti
ရွှိန		8000005056AA	x86_64 VM	knaas-cpe_2.23	.07 <u>vCPE-52</u>	CPE	Registered	Activated	Connected	Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
0		8000005056AA	x86_64 VM	knaas-cpe_2.23	07 VCPE-51	CPE	Registered	Activated	Connected	Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
P	. 🗆	8000005056AA	x86_64 VM	knaas-cpe_2.23	07 <u>vCPE-4</u>	CPE	Registered	Activated	Connected	Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
1		8000005056AA	x86_64 VM	knaas-cpe_2.23	07 vCPE-3	CPE	Registered	Activated	Connected	Supported	Yes	Demolab	Demolab	07/11/2023 17:42	1
\$		8000005056AA	x86_64 VM	knaas-cpe_2.23	.07 <u>vGW-12</u>	Gateway	Registered	Activated	Connected	Supported	Yes	Demolab	Demolab	26/10/2023 16:08	1
-	. 🗆	8000005056A/	x86_64 VM	knaas-cpe_2.23	.07 <u>vGW-11</u>	Gateway	Registered	Activated	Connected	Supported	Yes	Demolab	Demolab	26/10/2023 16:06	
0															
()															
Ō															
,															

Name	(Transnor	t Tenent		UNIT	emplate		Location			Antione
VCPE	3	Demola	b	~	UNIT	emplate	~	Sokolniki Parl	Modems		Delete
Device	PID	Custome	r Tenant		CPE 1	Template		Moscow, Cen Russia	Tunnels		Set location
8000	005056AAC4FD	Demola	b	~	VCP	PE-3	~		Multipathin	g	Show password
Descrip	tion								Activation	_	Get Activation URL Unregister CPE
									Deactivatio	n	Open Console
									Log files		Apply configurations
Device Model	Info SW Version		Controller	Gateways	User	Registered	Update	Management IP	State	Connection	Reboot Shutdown Export SD-WAN Configurat Export Network Settings
x86_64 VM	knaas- cpe_2 23.03.release.33.bios.a	nd64	10.50114:6653	-	admin	18/05/2023 15:27	29/06/2023 11:14	10.11.12.74	Activated	Connected	
Out of	Band Management										
				Charles		1.000	la data		~		

Отобразится список построенных туннелей с vCPE-3. В данном сценарии балансировка будет производится между туннелями с одинаковой стоимостью, без использования multi-weight. Значение стоимости отображается в столбце Cost вкладки Tunnels. Проверить значение стоимости туннелей: для работы балансировки у туннелей должно быть одинаковое значение стоимости.

										\approx	Sav	e Close
Configuration	Monitoring Problems E	ncryption Servic	e requests Thresholds	Tags Scr	Errors/sect	ettings Topo	Latency	Jitter (ms.)	More 🔻	Speed	Cost	\$ Q
			monitoring			(%)	(ms.)		loss (%)	(MB/sec)		
CPE [vGW-11: 8000005056AA	S CPE [vCPE-3: 800000505	56AA(Y	Y	1500	0	0	0	0	0	1000	10000	Management
CPE [vGW-11: 8000005056AA	S CPE [vCPE-3: 800000505	56AA(N	Y	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005056AA	A(CPE [vGW-11: 800000505	56AAS Y	Υ	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005056AA	A(CPE [vGW-11: 800000505	56AAS N	Y	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005056AA	A(CPE [vGW-12: 80000050	56AAI Y	Y	1500	0	0	2	0	0	1000	10000	Management
CPE [vCPE-3: 8000005056AA	A(CPE [vGW-12: 80000050	56AAI N	Y	1500	0	0	1	0	0	1000	10000	Management
CPE [vGW-12: 8000005056AA	AI CPE [vCPE-3: 800000505	56AACY	Y	1500	0	0	1	0	0	1000	10000	Management
CPE [vGW-12: 8000005056AA	AI CPE [vCPE-3: 800000505	56AA(N	Υ	1500	0	0	1	0	0	1000	10000	Management

3.1.5. Генерация тестового трафика.

Для генерации трафика между vCPE-3 и vCPE-4 на рабочих станциях wst3 и wst4 используется iperf.

Запустить сервер iperf на рабочей станции wst4:

[root@wst4]# iperf3 -s

[ivpanin@wst4 ~]\$ iperf3 -s

Server listening on 5201

Запустить клиент iperf на рабочей станции wst3:

[root@wst3]# iperf3 -u -t 6000 -c 10.20.4.11

[ivpanin@wst3 ~]\$ iperf3 -u -t 6000 -c 10.20.4.11 Connecting to host 10.20.4.11, port 5201 [4] local 10.20.3.11 port 54906 connected to 10.20.4.11 port 5201 ID] Interval Transfer Bandwidth Total Datagrams 116 KBytes 950 Kbits/sec 4] 4] 4] 1.05 Mbits/sec 1.04 Mbits/sec 1.00-2.00 129 KBytes 127 KBytes 3.00-4.00 129 KBytes 1.05 Mbits/sec 4

3.1.6. Проверка балансировки трафика между WAN интерфейсами CPE. Перейти в меню СРЕ, открыть vCPE-3. SD-WAN + CPE + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + Firmware Certificate >> C Export to CSV CPE 0 All © Waiting © Configuration - Registered © Registering - Error - Unknown All time Last year Last month Last week Last day 14/11/202310.41 - 14/11/202310.41 = All 6 · Connected 6 · Disconnected 0 · Connection error 0 Need update 0 ŝ ø Transport tenant : Customer tenant : Registered 🛞 Q 🔻 Actions * DPID Model SW version Name Role Status State Connection Fragmentation Usage 0 8000005056AA x86_64 VM knaas-cpe_2.23.07 vCPE-52 CPE Registered Activated Connected Supported Yes Demolab Demolab 07/11/2023 17:43 ရှိန (07/11/2023 17:43 8000005056AA x86_64 VM knaas-cpe_2.23.07 vCPE-51 CPE Registe ed Activated Connected Yes Demolab Demolab ы R 8000005056AA x86_64 VM knaas-cpe_2.23.07 vCPE-4 CPE Regist Demolal Demolab 07/11/2023 17:43 ≣ 8000005056AA x86_64 VM knaas-cpe_2.23.07 vCPE-3 CPE Registered Activated Connected Supported 07/11/2023 17:42 Yes Demolab Demolab 0 Ģ x86 64 VM knaas-cpe 2.23.07 vGW-12 റ്റ 8000005056A/ x86_64 VM knaas-cpe_2.23.07 vGW-11 Gateway Registered Activated Connected Supported Yes Demolab Demolab 26/10/2023 16:06 ÷ n 9 E. Открыть вкладку Monitoring. C A Not secure | https://10.0.1.11/sdwan/cpe/inventory $\leftarrow \rightarrow$ A ☆ SD-WAN +CPE Device + CPE Template + UNI template + SD-WAN Instance template + SD-WAN Instances Pool 4 Firmware Certificate + \gg \oslash Update Configurat Close vCPE-3 Configuration = Monitoring Ш. Problems Encryption Service requests Tags More к 6 Name sport Tenant UNI template Actions vCPE-3 Demolab Delete ø 0 Set location Device PID CPE Template Customer Tenant Deactivate (8000005056AAC4FD Demolab vCPE-3 Show password ရှိန ы Get Activation URL Location Description Sokolniki Park, Sokolniki District, Unregister CPE ≔ Moscow, Central Federal District, Open Console 친 Russia Open WEB Conso \bigcirc Apply configurations ട്ട് Ģ Reboot Shutdown Device Info Ŋ Export SD-WAN Configuration Manag æ Model SW Version Controller Gateways User Registered Update Export Network Settings IP Выбрать интерфейс eth0 и убедится на графике, что трафик проходит именно через него – всплеск на графике "Interface eth0: Bit sent[avg]". Для отображения данных необходимо подождать накопления статистики в течении 10 минут.

U000005056A	figuration Monito	rface eth0: Network	Manage I	vice requests Tag	s Configuration	IS SD-WAN	Settings Topol	6/2023 16:19	- 29/06/2023 17:	19 Real-time Day	Week Mo
4 mbps 1 mbps 683.59 kbps 8 kbps											
0 bps 16:19 29-06 Interfa Interfa Interfa Interfa Interfa	16:24 29-06 icce eth0: Bits recein icce eth0: Bits sent [icce eth0: Outbound icce eth0: Inbound p icce eth0: Outbound	16:29 29-06 ved [avg] avg] packets with errors [av packets with errors [av	16.34 29-06 35.56 k 1.25 mb avg] 0 g] 0 vg] 0	16:39 29-06 Average pps 40:33 kbps ps 132.9 kbps 0 0 0 0	16:44 29:06 Max 63:29 kbps 1.25 mbps 0 0 0	16:49 29-06	16:54 29-06	16:59 29-06	17.04 29-06	17.09 29-06	17:18 29-06

3.1.7. Проверка прохождения трафика через второй WAN интерфейс CPE.

Выбрать интерфейс *eth1* и убедится на графике, что трафик проходит через данный сетевой интерфейс.

	Registered E-3	nitoring Prob	lems Encry	otion Service r	equests Tags	More •		Update Configurat	ion Close
800005056AA	C4FD V	nterface eth1: N	etworktı 🗸				C 2	3/06/2023 11:52	- 23/06/2023 12:37
Manage Host								Real-time	Day Week Month
2.48 mbps									
1.86 mbps									
1.24 mbps									
634.77 kbps									
0 bps	12:04	12:00	12-14	12-10	12-24	12-20	10:34	10-30	12:50
23-06	23-06	23-06	23-06	23-06	23-06	23-06	23-06	23-06	23-06
■ Interfa	ce eth1: Bits rec	eived [avg]		Current 35.53 kbps	Average 26.45 kbps	Max 36.64 kbps			
■ Interfa	ce eth1: Bits sen	it [avg]	orroro [ov/5]	2.41 mbps	463.13 kbps	2.41 mbps			
Interface	ce ethi: Outbour ce ethi: Inbour	nu packets with er	rors [avg]	0	0	0			
Interface	ce eth1: Outbou	nd packets disca	arded [avg]	0	0	0			

Как видно из графиков в п. 3.1.6 и 3.1.7, в работе участвуют оба WAN интерфейса vCPE-3, и между ними выполняется балансировка трафика.

3.1.8. Возврат настроек после завершения теста

Выполнить п. 3.1.3 и изменить режим балансировки на per-flow.

Остановить процессы iperf на wst3 и wst4, запущенные в пункте 3.1.5 (возможно прервать с помощью Ctrl+Z).

3.2. Резервирование каналов связи в режиме Active/Standby.

В данном разделе рассматривается сценарий резервирования каналов связи в режиме Active/Standby для устройства vCPE-3. Для приоритезации WAN интерфейса используется параметр Cost, на резервном туннеле значение параметра будет увеличено по сравнению с основным. Генерация трафика на рабочих станциях wst3 и wst4 будет производится с помощью генератора трафика iperf. Для проверки работы резервирования будет использоваться встроенная в решение SD-WAN система мониторинга. Демонстрация работы резервного канала будет производится путем выключения основного WAN-интерфейса CPE.

3.2.1. Отображение списка туннелей vCPE-3 со смежными CPE устройствами.

Перейти в меню СРЕ и выбрать vCPE-3.

>>	_ c	PE											C	Export
<u>ш</u> 6	A	II c Waiting c Conf II 6 • Connected 6 •	iguration · Disconnect	Registered ed 0 • Conr	c Registering nection error 0	• Error Need up	- Unknown date 0	All time La	styear Lastmont	h <u>Lastweek L</u>	ast day 14/		14/11/2023 10:41	
¢ ,		DPID	Model	SW version	Name	Role	Status	State Conne	ction Fragmentat	ion: Usage :	Transport tenar	nt : Customer tenar	nt: Registered 🛞 Q.*	Action
ရှိဖွ	•	8000005056AA	x86_64 VM	knaas-cpe_2.	23.07 vCPE-52	CPE	Registered	Activated Conne	cted Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
0	1.1	8000005056A/	x86_64 VM	knaas-cpe_2.	23.07 VCPE-51	CPE	Registered	Activated Conne	cted Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
£	1	8000005056A/	x86_64 VM	knaas-cpe_2.	23.07 <u>vCPE-4</u>	CPE	Registered	Activated Conne	cted Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
, ,	•	8000005056A/	x86_64 VM	knaas-cpe_2.	23.07 <u>vCPE-3</u>	CPE	Registered	Activated Conne	cted Supported	Yes	Demolab	Demolab	07/11/2023 17:42	
1		8000005056A/	x86_64 VM	knaas-cpe_2.	23.07 <u>vGW-12</u>	Gateway	Registered	Activated Conne	cted Supported	Yes	Demolab	Demolab	26/10/2023 16:08	
2	•	8000005056A/	x86_64 VM	knaas-cpe_2.	.23.07 <u>vGW-11</u>	Gateway	Registered	Activated Conne	cted Supported	Yes	Demolab	Demolab	26/10/2023 16:06	
ейт	ин	а вкладк	y Tur	nnels	i.							↓ Upda	te Configuration	Close
ейт	пн	а вкладк vCPE-3 Configuration Mont	y Tur	nnels	-	rvice reque	sts Tags	Configurations	SD-WAN Setting	s Topology R	Aore *	V Upda	te Configuration	Close
ейт	ГИН	а вкладк vCPE-3 Configuration Moni	y Tur toring Pro	Diems En	icryption Se	rvice reque	sts Tags UNI te	Configurations	SD-WAN Setting	s Topology L Location	Aore *	🔆 Upda	te Configuration Actions	Close
ейт		а вкладк vCPE-3 Configuration Mon		Dilema En ansport Tena Demolab	. See	rvice reque	sta Taga UNI te	Configurations	SD-WAN Setting	s Topology Location Sokolniki Pari, Moscow, Cer	Aore * Modems Tunnels	Vpda	te Configuration Actions Delete Set location	Close
РЕЙТ	M H	а вкладк vCPE-3 Configuration Moni	y Tur	Demolab Demolab	ncryption <u>Se</u> ant	rvice reque	sts Tags UNI te CPE T VCPI	Configurations mplate emplate E-3	SD-WAN Setting	 Topology Location Sokolniki Parl Moscow, Cen Russia 	Acre * Modems Tunnels Multipathin	y Upda	te Configuration Actions Delete Set location Deactivate Show password	Close
ейт	ти н те сре-3 vice PID оосорбо	а вкладк vCPE-3 ^{Degistered} Configuration Moni 256AAC4FD	y Tur	oblems En ansport Tena Demolab Justomer Tena Demolab	cryption See ant	rvice reque	sts Tags UNI te CPE T VCPI	Configurations mplate emplate 5-3	SD-WAN Setting	s Topology D Location Sokolniki Pari Moscow, Cer Russia	Modems Tunnels Multipathin Activation	S Upda	Actions Delete Set location Deactivate Show password Get Activation URL	Close
ейт Nar VC Dev 80	me CPE-3 vice PID 0000050	а вкладк vCPE-3 Configuration Moni	y Tur	Demolab Demolab	eryption Se ant	rvice reque	UNI te CPE T VCPI	Configurations mplate emplate E-3	SD-WAN Setting	s Topology Location Sokolniki Parl Moscow, Cen Russia	Acre * Modems Tunnels Multipathin Activation Desctivatio	Upda	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console	Close
ейт ш Nar v Br Bee	CPE-3 vice PID 00000050	а вкладк vCPE-3 Configuration Mont		Demolab Demolab	int Second	rvice reque	sta Taga UNI te CPE T VCPI	Configurations mplate emplate E-3	SD-WAN Setting	s Topology Location Sokolniki Parti Moscow, Cen Russia	Acre * Modems Tunnels Multipathin Activation Desctivatio	& Upda	te Configuration Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console	Close
ейт Nar vc Bes	TO H	а вкладк vCPE-3 Configuration Moni		oblema En ansport Tena Demolab	ncryption See	rvice reque	eta Taga UNI te CPE T VCPI	Configurations mplate emplate =-3	SD-WAN Setting	Topology Location Sokolniki Pari Moscow, Cen Russia	Nore * Modems Tunnels Multipathin Activation Desctivatio Log files	y Upda	te Configuration Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations Reboot	Close
ейт Nar V Dev Be Des	TH H	а вкладк vCPE-3 Configuration Moni		oblems En ansport Tena Demolab	cryption See ant	vvice reque	Sts Tags UNI te CPE T VCPI	Configurations mplate emplate 5-3	SD-WAN Setting	s Topology D Location Sokolniki Pari Moscow, Cer Russia	Modems Tunnels Multipathin Activation Desctivatio Log files	Vipda	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con	Close s
ейт Nar V Dev B(C Dev Dev Moi	TO HA	A BKNAJK		oblema En ansport Tena Demolab Demolab	ant ant	vvice reque v	UNI te UNI te VCPI USer	Configurations mplate emplate 5-3 Registered	SD-WAN Setting	a Topology Location Sokolniki Parl Moscow, Cen Russia Management IP	Acre * Modems Tunnels Multipathin Activation Desctivatio Log files State	& Upda	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con Export SD-WAN Con	Close s s
Dev Moro X86 VM	me CPE-3 vice PID 00000506 acription	A BKNAJK	y Tur	oblema En ansport Tena Demolab Demolab Cor 4 10.5	ant solution see	Gateways	uni te Uni te CPE T VCPI User admin	Configurations mplate emplate E-3 Registered 18/05/2023 15.27	SD-WAN Setting	a Topology Location Sokolniki Parl Russia Management IP	Acre * Modems Tunnels Multipathin Activation Desctivatio Log files State Activated	& Upda	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con Export Network Sett	Close s s
Period Marine Des Morine X86 VM Out	me CPE-3 vice PID 00000505 scription	A BKNAQK	y Tur	Demotab Demotab Demotab Justomer Tena Demotab Corr 4	eryption Se ant ant ntroller 50.114: 6653	Crvice reque	uni te CPE T VCPI User admin	Configurations mplate emplate 2-3 Registered 18/05/2023 15.27	SD-WAN Setting	Topology Location Sokolniki Part Moscow, Cen Russia Management IP	Aore * Modems Tunnels Multipathin Activation Desctivatio Log files State Activated	& Upda	te Configuration Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configuration: Reboot Shutdown Export SD-WAN Con Export Network Sett	Close \$ \$

На вкладке Tunnels представлен список построенных туннелей выбранного СРЕ со смежными СРЕ устройствами. В столбцах Source и Destination указаны СРЕ устройства источника и назначения однонаправленного туннеля. Номер порта указывает на номер WAN интерфейса СРЕ устройства. Номер порта назначается по порядку, начиная с порта 4800, по одному на каждый WAN интерфейс. Порт 4800 означает WAN интерфейс sdwan0 (eth0), порт 4801 означает WAN интерфейс sdwan1 (eth1).

										≈ [Save	Close
Configuration Monit	oring Problems Encryption Ser	vice requests Tags Sc	ripts SD-WAN	settings 1	opology Network	settings BGF	esettings OSPF	Routing Fil	ters More *			
Source	Destination	Unsolicited :	Thresholds monitoring	MTU ⑦	Errors/second	Utilization (9	%) Latency (ms.)	Jitter (ms.)	Packet loss (%)	Speed (MB/sec)	Cost	
CPE [vGW-11: 8000005056AA9EA	6] 4800 CPE [vCPE-3: 80000050564	AAC4FD] :4800 Y	Y	1500	0	0	0	0	0	1000	10000	Managem
CPE [vGW-11: 8000005056AA9EA	5] 4800 CPE [vCPE-3: 80000050564	AAC4FD]:4801 N	Y	1500	0	0	0	0	0	1000	10000	Managem
CPE [vCPE-3: 8000005056AAC4F	D]: 4800 CPE [vGW-11: 8000005056A	A9EA5]: 4800 Y	Y	1500	0	0	0	0	0	1000	10000	Managem
CPE [vCPE-3: 8000005056AAC4F	D]: 4801 CPE [vGW-11: 8000005056A	A9EA5]: 1800 N	Y	1500	0	0	0	0	0	1000	10000	Managem
CPE [vCPE-3: 8000005056AAC4F	D] : 4800 CPE [vGW-12: 80000050564	AD2B1]: 4800 Y	Y	1500	0	0	2	0	0	1000	10000	Managem
CPE [vCPE-3: 8000005056AAC4F	D]: 4801 CPE [vGW-12: 80000050564	AD2B1]: 4800 N	Y	1500	0	0	1	0	0	1000	10000	Managem
CPE [vGW-12: 8000005056AAD2B	1]: 4800 CPE [vCPE-3: 80000050564	AC4FD]: 4800 Y	Y	1500	0	0	1	0	0	1000	10000	Managem
CPE [vGW-12: 8000005056AAD2B	1] 4800 CPE [vCPE-3: 80000050564	AC4FD]:4801 N	Y	1500	0	0	1	0	0	1000	10000	Managem

3.2.2. Настройка значения стоимости (Cost) для всех туннелей, построенных через резервный (Standby) WAN интерфейс (sdwan1/eth1) устройства vCPE-3.

В решении SD-WAN топологией по умолчанию является звезда, поэтому трафик между CPE проходит через шлюзы. В данном сценарии будет увеличена стоимость туннелей, проходящих через резервный WAN-интерфейс (sdwan1/eth1) vCPE3, между vCPE-3 и шлюзами vGW-11 / vGW-12.

Найти все туннели между vCPE-3 и vGW-11 / vGW-12, построенные через второй WAN интерфейс vCPE-3, порт 4801:

- vCPE-3:4801 <--> vGW-11:4800
- vCPE-3:4801 <--> vGW-12:4800
- vGW-11:4800 <--> vCPE-3:4801
- vGW-12:4800 <--> vCPE-3:4801

Поочередно нажать Management > Set Cost.

										💥 Save	e Close
Configuration Monitoring	Problems Encryption Service reque	sts . Tags . Scri	ots SD-WAN se	ttings To	pology Network se	ttings BGP se	ttings OSPF	Routing Filter	More •		
Source	Destination :	Unsolicited	Thresholds monitoring	MTU ⊘	Errors/second	Utilization (%)	Latency (ms.)	Jitter (ms.)	Packet loss (%)	Speed (MB/sec)	Cost
CPE [vGW-11: 8000005056AA9EA5] : 48	00 CPE [vCPE-3: 8000005056AAC4FD] : 4	800 Y	Y	1500	0	0	0	0	0	1000	10000 Managemi
CPE [vGW-11: 8000005056AA9EA5] : 48	00 CPE [vCPE-3: 8000005056AAC4FD] : 4	801 N	Y	1500	0	0	0	0	0	1000	Set cost
CPE [vCPE-3: 8000005056AAC4FD] : 48	00 CPE [vGW-11: 8000005056AA9EA5] : 4	800 Y	Υ	1500	0	0	0	0	0	1000	Set monitoring threshold
CPE [vCPE-3: 8000005056AAC4FD] : 48	01 CPE [vGW-11: 8000005056AA9EA5] : 4	800 N	Υ	1500	0	0	0	0	0	1000	Set encryption
CPE [vCPE-3: 8000005056AAC4FD] : 48	00 CPE [vGW-12: 8000005056AAD2B1] : 4	800 Y	Υ	1500	0	0	2	0	0	1000	Set dampening
CPE [vCPE-3: 8000005056AAC4FD] : 48	01 CPE [vGW-12: 8000005056AAD2B1] : 4	800 N	Y	1500	0	0	1	0	0	1000	Set FEC/reordering
CPE [vGW-12: 8000005056AAD2B1] : 48	00 CPE [vCPE-3: 8000005056AAC4FD] : 4	800 Y	Y	1500	0	0	1	0	0	1000	Clear statistics
CPE [vGW-12: 8000005056AAD2B1] : 48	00 CPE [vCPE-3: 8000005056AAC4FD] : 4	801 N	Y	1500	0	0	1	0	0	1000	Check MTU

Увеличить значение стоимости (по умолчанию 10000):

- В поле Cost задать значение 900000.
- Отметить Override переопределить значение стоимости.
- Both links применить настройки к обоим линкам между парой СРЕ устройств.

🗹 Override
Save for both tunnel
Save



3.2.3. Генерация трафика для демонстрации работы Active/Standby на WAN интерфейсах CPE.

Для генерации трафика между vCPE-3 и vCPE-4 на рабочих станциях wst3 и wst4 будет использоваться iperf.

Запустить сервер iperf на wst4:

[root@wst4]# iperf3 -s

ivpanin@wst4 ~]\$ iperf3 -s

Запустить клиент iperf на wst3:

[root@wst3]# iperf3 -u -t 6000 -c 10.20.4.11

[ivpanin@wst3 ~]\$ ipe:	rf3 -u -t 6000 -	-c 10.20.4.11	
Connecting to host 10	.20.4.11, port S	5201	
[4] local 10.20.3.1	l port 54906 com	nnected to 10.20.	4.11 port 5201
[ID] Interval	Transfer	Bandwidth	Total Datagrams
[4] 0.00-1.00 se	ec 116 KBytes	950 Kbits/sec	82
[4] 1.00-2.00 se	ec 129 KBytes	1.05 Mbits/sec	
[4] 2.00-3.00 se	ec 127 KBytes	1.04 Mbits/sec	90
[4] 3.00-4.00 se	ec 129 KBytes	1.05 Mbits/sec	

3.2.4. Проверка статистики трафика на WAN интерфейсах в системе мониторинга.

Перейти в меню СРЕ, выбрать vCPE-3. Открыть вкладку Monitoring. Выбрать интерфейс *eth0* и убедится на графике, что трафик проходит через него.



Выбрать интерфейс *eth1* и убедиться на графике (кривая "Interface eth0: Bit sent[avg]") в том, что через данный интерфейс не проходит сетевой трафик.





3.2.5. Эмуляция отказа основного WAN-интерфейса.

Подключиться к маршрутизатору isp и отключить сетевой интерфейс, к которому подключен сетевой интерфейс sdwan0 (eth0) устройства vCPE-3:

[root@isp]# ifconfig ens161 down

```
gr roote10.100.0.2's password:
Last failed login: Fri Jun 23 13:54:45 MSK 2023 from 10.160.0.10 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Thu May 18 14:59:19 2023 from 10.160.0.10
[root08:p -]# ifconfig ensl61 down
```

Из-за особенности работы iperf возможно потребуется перезапустить iperf3 клиент на wst-3: п. 3.2.3

3.2.6. Проверка работы резервирования WAN интерфейсов в системе мониторинга.

Перейти в меню СРЕ и выбрать vCPE-3. Открыть вкладку Monitoring. Выбрать интерфейс *eth1* и убедиться на графике, что трафик переключился на данный сетевой интерфейс.

VC <u>Cc</u> 8000005056	Registere PE-3 onfiguration	Monitoring P	roblems Encry	yption Servic Manage Hos	e requests st	Tags	Configurations	SD-WAN Settings	3 Topolog 29/06/	<u>y</u> <u>More</u> ▼ 202316:24	- 29/06/2023 17	Update Con	figuration	Close	Nonth
2.48 mbps 1.86 mbps 1.24 mbps 634.77 kbps													/		
0 bps 16:25 29-06 Inter Inter Inter Inter Inter Inter	16:29 29-06 fface eth1: Bits r fface eth1: Bits s fface eth1: Outb fface eth1: Inbou fface eth1: Inbou	16:33 29-06 received [avg] sent [avg] yound packets witt yound packets witt yound packets disc	16:37 29-06 vith errors [avg] h errors [avg] iiscarded [avg] carded [avg]	16:41 29-06 Current 56:59 kbps 2.46 mbps 0 0 0 0	16:45 29-06 Avera 58 kb 392.4 0 0 0 0 0	16:49 29-06 ps 2 kbps	16:53 29:06 Max 63:12 kbps 2.46 mbps 0 0 0 0 0	16:57 29-06	17:01 29-06	17:05 29-06	17:09 29-06	17:13 29-06	17:17 29-06	17:23 29-06	

3.2.7. Возврат настроек после завершения теста.

Включить сетевой интерфейс на хосте isp, отключенный в п.3.2.5.

[root@isp]# ifconfig ens161 up

Вернуть значение стоимости туннелей, измененное в п. 3.2.2, на значение по умолчанию.

Остановить процессы iperf на wst3 и wst4, запущенные в п. 3.2.3 (возможно прервать с помощью Ctrl+Z).

3.3. Резервирование каналов связи в широковещательном (broadcast) режиме.

Kaspersky SD-WAN обеспечивает защиту от перерывов связи с устройствами CPE с помощью одновременного использования доступных каналов передачи данных. Для достижения дополнительной отказоустойчивости поддерживается широковещательный (broadcast) режим балансировки – копии пакетов передаются одновременно во все туннели для исключения потерь.



Рисунок 3.3.1 Дублирование пакетов

Для получения дополнительной информации о резервировании каналов связи обратитесь к Kaspersky SD-WAN Online Help > Резервирование каналов передачи данных между устройствами CPE: <u>https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/239053.htm</u>

В данном разделе рассматривается сценарий резервирования между туннелями устройства vCPE-3. Для этого будет использоваться режим балансировки пакетов в режиме Broadcast. В данном режиме CPE отправляет копии пакетов одновременно по всем доступным туннелям.

Для демонстрации резервирования трафика между vCPE-3 и srv1 на хостах wst3 и srv1 используется ICMP ping. Для проверки работы механизма дублирования будет использоваться tcpdump на vCPE-3.

3.3.1. Выбор режима балансировки для транспортного сервиса. Настройка режима broadcast для транспортного сервиса.

Доступные режимы балансировки:

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

Для выбора режима балансировки перейти в меню Infrastructure > SD-WAN контроллер > Management > Open configuration menu.



Перейти в раздел с транспортными сервисами M2M. Выбрать транспортный сервис для редактирования, нажать Management > Edit.



29

Нажать Next, Next и Save.

OFI

Cancel



3.3.3. Проверка работы режима балансировки broadcast у транспортного сервиса.

Открыть 2 SSH сессии до vCPE-3.

Запустить tcpdump на туннельных интерфейсах: в 1й сессии на genev_sys_4800, во 2й – на genev_sys_4801:

tcpdump -i genev_sys_4800 | grep 10.1.1.11 # tcpdump -i genev_sys_4801 | grep 10.1.1.11

10.1.1.11 – адрес хоста srv1.

genev_sys – туннельные интерфейсы СРЕ. Номер порта указывает на номер WAN интерфейса СРЕ устройства. Номер назначается по порядку, начиная с порта 4800, по одному на каждый WAN интерфейс. Порт 4800 означает WAN интерфейс sdwan0 (eth0), порт 4801 означает WAN интерфейс sdwan1 (eth1).



Запустить ICMP ping c wst3 до srv1:

ping 10.1.1.11

[ivpanin@wst3 ~]\$ ping 10.1.1.11

PING 10.1.1.11 (10.1.1.11) 56(84) bytes of data. 64 bytes from 10.1.1.11: icmp_seq=1 ttl=61 time=3.53 ms 64 bytes from 10.1.1.11: icmp_seq=2 ttl=61 time=2.48 ms 64 bytes from 10.1.1.11: icmp_seq=3 ttl=61 time=2.29 ms 64 bytes from 10.1.1.11: icmp_seq=4 ttl=61 time=2.49 ms 64 bytes from 10.1.1.11: icmp_seq=5 ttl=61 time=2.18 ms 64 bytes from 10.1.1.11: icmp_seq=6 ttl=61 time=2.57 ms

В выводе tcpdump на vCPE-3 появятся ICMP пакеты. Видно, что на каждый интерфейс была отправлена копия пакетов (у пакетов одинаковый sequence).



🧬 root@8000005056AAC4FD: ~	-	□ ×	
12:23:12.356066 IF 10.20.3.11 > 10.1.11: ICMM echo request, id 2372), set 12:23:12.35616 IF 10.1.11 > 10.20.3.11: ICMM echo request, id 23720, set 12:23:13.441765 IF 10.2.0.3.11 > 10.2.0.3.11: ICMM echo request, id 23720, set 12:23:14.526531 IF 10.2.0.3.11 > 10.2.0.3.11: ICMM echo request, id 23720, set 12:23:14.526531 IF 10.2.0.3.11 > 10.2.0.3.11: ICMM echo request, id 23720, set 12:23:14.530783 IF 10.2.0.3.11 > 10.1.1.11: ICMM echo request, id 23720, set 12:23:15.617116 IF 10.1.1.11 > 10.20.3.11: ICMM echo request, id 23720, set 12:23:15.617116 IF 10.1.1.11 > 10.20.3.11: ICMM echo request, id 23720, set 12:23:16.6999 IF 10.2.0.3.11 > 10.1.11: ICMM echo request, id 23720, set 12:23:16.6999 IF 10.2.0.3.11 > 10.1.11: ICMM echo request, id 23720, set 12:23:16.699276 IF 10.1.1.11 > 10.20.3.11: ICMM echo request, id 23720, set 12:23:17.673433 IF 10.2.3.11 > 10.2.0.3.11: ICMM echo request, id 23720, set 12:23:17.787437 IF 10.1.1.11 > 10.20.3.11: ICMM echo request, id 23720, set 12:23:17.787437 IF 10.1.1.11 > 10.20.3.11: ICMM echo request, id 23720, set	eq 1, le 1, leng eq 2, le 2, leng eq 3, le 3, leng eq 4, le 4, leng eq 5, le 5, leng eq 6, leng	ngth 64 th 64 ingth 64 th 64 ingth 64 ingth 64 ingth 64 ingth 64 ingth 64 ingth 64 ingth 64 ingth 64	12:23:12.356946 IF 10.20.3.11 > 10.1.1.11: ICMP echo request, id 2372, seq 1, length 64 12:23:12.359166 IF 10.1.1.11 > 10.20.3.11: ICMP echo request, id 23720, seq 1, length 64 12:23:13.447851 IF 10.2.3.11: 10.20.3.11: ICMP echo request, id 2372, seq 2, length 64 12:23:13.647851 Pt 10.1.1.11: 10.20.3.11: ICMP echo request, id 23720, seq 2, length 64 12:23:14.53693 IF 10.2.3.11: 10.20.3.11: ICMP echo request, id 23720, seq 3, length 64 12:23:14.536799 IF 10.3.1.1.11: ICMP echo request, id 23720, seq 3, length 64 12:23:14.536799 IF 10.3.1.1.1.11: ICMP echo request, id 23720, seq 4, length 64 12:23:15.617186 IF 10.1.1.1: 10.20.3.11: ICMP echo request, id 23720, seq 4, length 64 12:23:15.667858 IF 10.2.3.11: 10.1.1.11: ICMP echo request, id 23720, seq 5, length 64 12:23:17.78382 IF 10.1.1.1: 10.20.3.11: ICMP echo request, id 23720, seq 5, length 64 12:23:17.78382 IF 10.2.3.11: 10.1.1.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: 10.1.1.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 12:23:17.78382 IF 10.2.3.11: ICMP echo request, id 23720, seq 6, length 64 I2:23:17.78382 IF 10.2.3.11: ICMP echo re

3.3.4. Возврат настроек после завершения теста.

Выполнить п. 3.3.2 и изменить режим балансировки на per-flow.

Остановить ICMP ping на wst3, запущенный в пункте 3.3.3 (возможно прервать с помощью Ctrl+Z).

3.4. Повышение надежности каналов с использованием механизма Forward Error Correction (FEC).

Функция Forward Error Correction (далее также FEC) позволяет восстанавливать принимаемые данные на устройстве СРЕ при наличии потерь на каналах передачи данных. Восстановление данных обеспечивается избыточным кодированием потока данных на устройстве, находящемся на передающей стороне.

Передающее устройство СРЕ кодирует поток выходящих в туннель пакетов трафика с добавлением избыточных пакетов. Степень избыточности можно настроить через параметры контроллера SD-WAN или на отдельном туннеле.

Принимающее устройство СРЕ буферизует принятые через туннель пакеты трафика и декодирует их с восстановлением потерянных пакетов, если это возможно.



Рис. 3.4.1 Forward Error Correction (FEC)

Использование FEC снижает влияние повышенного показателя потерь пакетов трафика на каналах передачи данных, особенно для UDP-приложений, а также уменьшает количество вызывающих задержки повторных передач пакетов (англ. retransmissions) для TCP-сессий. Рекомендуется использовать FEC на так называемых noisy links (или зашумленных туннелях) для уменьшения коэффициента потери пакетов трафика и увеличения скорости TCP-соединений.

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help > Включение функции Forward Error Correction: <u>https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/245033.htm</u>

В данном сценарии рассматривается сценарий с эмуляцией потерь на канале, измерением качества туннелей и включением FEC для восстановления потерянных пакетов. Тестовый трафик будет генерироваться между рабочими станциями wst3 и srv1 с использованием ICMP пинг.

Эмуляция потерь будет проводиться на хосте isp с помощью системы Linux Traffic Control (TC).



3.4.1. Генерация тестового трафика.

Запустить icmp ping c хоста wst3 до srv1:

[root@wst3]# ping 10.1.1.11

```
[ivpanin@wst3 ~]$ ping 10.1.1.11
PING 10.1.1.11 (10.1.1.11) 56(84) bytes of data.
64 bytes from 10.1.1.11: icmp_seq=1 ttl=61 time=11.5 ms
64 bytes from 10.1.1.11: icmp_seq=2 ttl=61 time=7.78 ms
64 bytes from 10.1.1.11: icmp_seq=3 ttl=61 time=5.69 ms
64 bytes from 10.1.1.11: icmp seq=4 ttl=61 time=3.68 ms
```

3.4.2. Эмуляция потерь пакетов с помощью ТС.

Для теста необходимо включить эмуляцию потерь на сетевом интерфейсе хоста isp, к которому подключен sdwan0 (eth0) интерфейс vCPE-3.

Подключиться к хосту isp и выполнить команду:

[root@isp]# tc qdisc add dev ens161 root netem delay 1ms 0ms limit 1250000 loss 5%

Данная команда создает 5% потерь (packet loss). Параметр delay настраивает задержку в 1ms с разбросом в 0ms, limit – выделяет буфер в 1250000 байт для обработки данных TC

Проверить примененные настройки с помощью следующей команды:

[root@isp]# tc qdisc show

[root(]isp ~]	# tc	qdi	.sc a	add dev	ens1	61 root	n	etem de	ela	ay 1ms Om	s]	Lim	it	12	250	000) 1	.os	5	10%				
[root(]isp ~]	# tc	qdi	SC S	show																				
qdisc	disc noqueue 0: dev lo root refcnt 2																								
qdisc	netem	8005:	: de	ev er	ıs161 r	oot re	efcnt 2	1	imit 12	25(0000 dela	y 1	L.O	ms	10	SS	10)응							
qdisc	pfifo	fast	0:	dev	ens192	root	refcnt	2	bands	3	priomap	1	2	2	2 1	2	0	0	1	1	11	1	1	1	1
qdisc	pfifo_	fast	0:	dev	ens193	root	refcnt	2	bands	3	priomap	1	2	2	2 1	2		0	1	1	11	1	1	1	1
qdisc	pfifo_	fast	0:	dev	ens224	root	refcnt	2	bands	3	priomap	1	2	2	2 1	2		0	1	1	11	1	1	1	1
qdisc	pfifo	fast	0:	dev	ens225	root	refcnt	2	bands	3	priomap	1	2	2	2 1	2		0	1	1	1 1	1	1	1	1
qdisc	pfifo	fast	0:	dev	ens256	root	refcnt	2	bands	3	priomap	1	2	2	2 1	2		0	1	1	1 1	1	1	1	1
qdisc	pfifo	fast	0:	dev	ens257	root	refcnt	2	bands	3	priomap	1	2	2	2 1	2		0	1	1	1 1	1	1	1	1
[root(]isp ~]	#																							

3.4.3. Проверка на рабочей станции wst3 потерь в статистике ping.

Примечание: по умолчанию режим балансировки per-flow (если он не был изменен на per-packet в 3.1), поэтому поток может пойти через другой интерфейс, и эмуляция потерь не применится на интерфейс, через который будет проходить поток трафика. В данном сценарии должен использоваться режим per-flow.

Как видно ниже по ICMP sequence number, присутствуют потери пакетов, видны пропущенные ответы (пропущены sequence 281, 290, 293).

64	bytes	from	10.1.1.11:	icmp_seq=275	ttl=61	time=29.8	ms
64	bytes	from	10.1.1.11:	icmp_seq=276	ttl=61	time=7.69	ms
64	bytes	from	10.1.1.11:	icmp_seq=277	ttl=61	time=5.76	ms
64	bytes	from	10.1.1.11:	icmp_seq=278	ttl=61	time=43.8	ms
64	bytes	from	10.1.1.11:	icmp_seq=279	ttl=61	time=21.8	ms
64	bytes	from	10.1.1.11:	icmp_seq=280	ttl=61	time=79.7	ms
64	bytes	from	10.1.1.11:	icmp_seq=282	ttl=61	time=17.6	ms
64	bytes	from	10.1.1.11:	icmp seq=283	ttl=61	time=15.8	ms
64	bytes	from	10.1.1.11:	icmp_seq=286	ttl=61	time=14.6	ms
64	bytes	from	10.1.1.11:	icmp_seq=287	ttl=61	time=12.8	ms
64	bytes	from	10.1.1.11:	icmp seq=288	ttl=61	time=10.7	ms
64	bytes	from	10.1.1.11:	icmp seq=289	ttl=61	time=28.7	ms
64	bytes	from	10.1.1.11:	icmp_seq=291	ttl=61	time=66.7	ms
64	bytes	from	10.1.1.11:	icmp_seq=292	ttl=61	time=4.65	ms
64	bytes	from	10.1.1.11:	icmp_seq=294	ttl=61	time=5.94	ms
64	bytes	from	10.1.1.11:	icmp_seq=295	ttl=61	time=41.5	ms
64	bytes	from	10.1.1.11:	icmp_seq=296	ttl=61	time=79.7	ms
64	bytes	from	10.1.1.11:	icmp_seq=297	ttl=61	time=17.7	ms
64	bytes	from	10.1.1.11:	icmp_seq=298	ttl=61	time=15.7	ms
64	bytes	from	10.1.1.11:	icmp_seq=300	ttl=61	time=13.8	ms
64	bytes	from	10.1.1.11:	icmp_seq=301	ttl=61	time=32.6	ms
64	bytes	from	10.1.1.11:	icmp_seq=302	ttl=61	time=11.7	ms

Если в статистике не будет видно потерь, то значит, что трафик идет через интерфейс, где не применена эмуляция потерь и необходимо на хосте isp применить эмуляцию на другой интерфейс:

[root@isp]# tc qdisc add dev ens193 root netem delay 1ms 0ms limit 1250000 loss 5%

и снять задержку с первого сетевого интерфейса:

[root@isp]# tc qdisc del dev ens161 root

3.4.4. Включение мониторинга потерь пакетов на туннелях.

Перейти в меню СРЕ и выбрать vCPE-3.

22	CPE										0	Expor
6 6	All c Waiting c Configu All 6 · Connected 6 · D	uration • I Disconnected	Registered c Registe	ring • Error or 0 Need upc	Unknown date 0	All time Last ye	ar Last month	Lastweek	Last day 14/1	/2023 10:41 -	14/11/2023 10:41	
¢.	DPID	todel S	SW version Nam	e Role	Status	State Connection	Fragmentati	on Usage	Transport tenan	t : Customer tenant	t: Registered 🛞 Q*	Actio
26	• 8000005056AA x8	86_64 VM k	knaas-cpe_2.23.07 vCPI	-52 CPE	Registered	d Activated Connected	Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
0	• 8000005056AA x8	86_64 VM k	knaas-cpe_2.23.07 vCPI	E-51 CPE	Registered	d Activated Connected	Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
£	• 8000005056AA x8	86_64 VM k	knaas-cpe_2.23.07 vCP	E-4 CPE	Registered	d Activated Connected	Supported	Yes	Demolab	Demolab	07/11/2023 17:43	
1	• <u>8000005056A</u> / x8	86_64 VM k	knaas-cpe_2.23.07 vCP	E-3 CPE	Registered	d Activated Connected	Supported	Yes	Demolab	Demolab	07/11/2023 17:42	
(g) 1	• 8000005056AA x8	86_64 VM k	knaas-cpe_2.23.07 VGW	-12 Gateway	Registered	d Activated Connected	Supported	Yes	Demolab	Demolab	26/10/2023 16:08	
Ł	• 8000005056A/ x8	86_64 VM k	knaas-cpe_2.23.07 vGW	-11 Gateway	Registered	d Activated Connected	Supported	Yes	Demolab	Demolab	26/10/2023 16:06	
0												
ि												
신다												
0												
-												
≣Ø												
1												
ейти	1 на вкладку	' Tun	nels.									
ейти	1 на вкладку	' Tun	nnels.							Vpdate	e Configuration	Close
ейти	1 На ВКЛАДКУ L vCPE-3 O Configuration Monito	ring Prot	nnels.	Service reque	sts Tags	Configurations SI)-WAN Settings	Topology	Mare *	Update	e Configuration	Close
ЭЙТИ	1 На вкладку vcpe-3 Configuration Monito	r Tun	Dimels.	Service reque	sts Tags UNI te	Configurations St)-WAN Settings	Topology	More *	Vpdate	2 Configuration	Close
ейти ш Name vCP5	1 На вкладку	r Tun	blems Encryption insport Tenant emolab	Service reque	ests Tags UNI te	Configurations SI	0-WAN Settings	Topology Location Sokolniki Pa	More *	Vpdate	2 Configuration Actions Delete	Close
	1 На вкладку vcPe-3 configuration Monito	r Tun	blems Encryption insport Tenant emolab stomer Tenant	Service reque	uni te	Configurations St emplate Femplate	D-WAN Settings	Topology Location Sokolniki Pa Moscow, Ce Russia	More * Modems I Tunnels		Actions Delete Set location Deactivate	Close
EXTR IIIII Name VCPE Device 8000	1 На вкладку vcPE-3 configuration Monito E-3 e PID 0005056AAC4FD	Y Tun	blems Encryption Insport Tenant emolab stomer Tenant emolab	Service reque	sts Tags UNI te CPE T VCP	Configurations St emplate Femplate E-3	D-WAN Settings	Topology Location Sokoliniki Pa Moscow, Ce Russia	More * Modems r Tunneis Multipathing		Configuration Actions Delete Set location Deactivate Show password	Close
Name vCPf Bevice 8000	1 На вкладку vcPe-3 configuration Monito e PID 0005056AAC4FD	r Tun	blems Encryption Insport Tenant emolab stomer Tenant emolab	Service reque	Sts Tags UNI te CPE T VCP	Configurations SI emplate Femplate E-3	-WAN Settings	Location Sokolniki Pa Moscow, Ce Russia	More * Modems Tunnels Multipathing Activation	Vipdate	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE	Close
EXTR IIII Name vCPf Boold Descri	1 НА ВКЛАДКУ VCPE-3 Configuration Monito E-3 e PID 00005056AAC4FD	ring Prot	blema Encryption Insport Tenant emolab stomer Tenant emolab	Service reque	UNI te UNI te VCP	Configurations St emplate Femplate E-3	-WAN Settings	Topology Location Sokolniki Pa Moscow, Ce Russia	More * Modems Tunnels Multipathing Activation Desctivatior	Update	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console	Close
Name VCPE Device 8000	1 На вкладку vcpe-3 Configuration Monito E-3 е PID 0005056AAC4FD iption	ring Prot	blema Encryption Insport Tenant emolab stomer Tenant emolab	Service reque	UNI te	Configurations SI emplate femplate E-3	D-WAN Settings	Topology Location Sokolniki Pa Moscow, Ce Russia	Modems Modems Tunnels Multipathing Activation Desctivation Log files	Vpdate	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations	Close
ЭЙТИ (IIII) Name vCPB Device 8000 Descri	1 На вкладку vcPE-3 Configuration Monito E-3 е PID 0005056AAC4FD iption	Y Tun	blem Encryption insport Tenant emolab stomer Tenant emolab	Service reque	UNI te	Configurations SI emplate femplate E-3	D-WAN Settings	Topology Location Sokolniki Pa Moscow, Ce Russia	More * Moderns Tunnels Multipathing Activation Deactivation Log files	Vpdate	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Apply configurations Reboot	Close
Pevicer Devicer	1 НА ВКЛАДКУ VCPE-3 Configuration Monito E-3 е PID 0005056AAC4FD iption	v Tun	blem Encryption Insport Tenant emolab stomer Tenant emolab	Service reque	UNI te	Configurations SI emplate femplate E-3	D-WAN Settings	Topology Location Sokolniki Pa Moscow, Ce Russia	More * Moderns Tunnels Multipathing Activation Desctivation Log files	Vpdate	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Apply configurations Reboot Shutdown Export SD-WAN Con	Close
Pevice Device Model	1 НА ВКЛАДКУ VCPE-3 Configuration Monito E-3 e PID 0005056AAC4FD iption	v Tun	blem Encryption insport Tenant emolab stomer Tenant emolab	Service reque	sts Tags UNI te CPE I VCP	Configurations SI emplate femplate E-3	D-WAN Settings	Topology Location Sokolniki Pa Moscow, Ce Russia Management IP	Moderns Moderns Tunnels Multipathing Activation Deactivation Log files State	S Update	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con Export Network Sett	Close
Linii Linii Name vcPf BOO Descri Model X86,6*	1 На ВКЛадку vcPE-3 Configuration Monito E-3 е PID 0005056AAC4FD iption e Info i SW Version 4 knaas- cpe,223.03 release 33.1:	v Tun	blema Encryption Insport Tenant emolab stomer Tenant emolab Controller 10.50.114: 665	Service reque Gateways 3 -	sta Taga UNI te CPE T VCP User admin	Configurations SI emplate Femplate E<-3	-WAN Settings	Topology Location Sokolniki Pa Moscow, Ce Russia Management IP	More * Moderns Tunnels Multipathing Activation Descrivation Log files State Activated	Update Connection Connected	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con Export Network Sett	Close
Name vCPE 8000 Device Model x86.6 VM	1 На ВКЛадку VCPE-3 Configuration Monito E-3 e PID 0005056AAC4FD iption e Info I SW Version 4 knass- cpe,223.03 release.33.b f Band Management	ring Prot Tra Du Du Dios.amdó4	blem Encryption insport Tenant emolab tomer Tenant emolab Controller 10.50 114 : 665	Service reque Gateways 3 -	ats Tags UNI te CPE T VCP	Configurations SI emplate E-3 Registered Up 18/05/2023 29 15.27 11:	D-WAN Settings	Topology Location Sokolniki Pa Masoaw, Ce Russia Management IP	Moderns Moderns Tunnels Multipathing Activation Desctivation Log files State Activated	S Update Connection	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con Export Network Sett	figurat
EWITH الالتان الاتان الالتان الالتان الاتان التان الاتان المان المان الاتان المان المان المان المان المان المان المان المان الاتان الاتان الاتان المان المان المان المان الاتان الاتان الاتان المان المان الات الاتان الاتان الاتان الات الات الاتان	1 На ВКЛадку VCPE-3 Configuration Monito E-3 e PID 0005056AAC4FD iption e Info i SW Version 4 knaas- cpe_223.03 release 33.b fBand Management	ring Prot Tra Du Cus Dios.amdó4	blems Encryption insport Tenant emolab stomer Tenant emolab Controller 10.50.114: 665	Service reque Gateways 3 - Status	sta Taga UNI te CPE T VCP	Configurations SI emplate E-3 Registered Up 18/05/2023 29 15.27 11: Last Upda	D-WAN Settings v v date /06/2023 4 te	Topology Location Sokolniki Pa Moscow, Ce Russia Management IP	Moderns Moderns Moderns Multipathing Activation Desctivation Log files State Activated	Update Update Connection Connected	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con Export Network Sett	figurat
EWITH Name VCPPI Bool Bool Bool Bool Bool Bool Bool Boo	1 На ВКЛадку VCPE-3 Configuration Monito E-3 e PID 0005056AAC4FD iption e Info i SW Version 4 knaas- cpe_223.03 release 33.b f Band Management	ring Prot	blems Encryption insport Tenant emolab stomer Tenant emolab Controller 10.50.114: 665	Service reque Cateways 3 - Status Comple	eted	Configurations SI emplate E-3 Registered Up 18/05/2023 29 15.27 11: Last Upda 15/06/202	D-WAN Settings voidate /06/2023 4 te 13 16 29	Topology Location Sokolniki Pa Moscow, Ce Russia Management IP	Moderns Moderns Moderns Multipathing Activation Desctivatior Log files State Activated	Update Update Connection Connected	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con Export SD-WAN Con	Close
Line Control C	1 НА ВКЛАДКУ VCPE-3 Configuration Monito E-3 e PID 0005056AAC4FD iption e Info i SW Version 4 knaas- cpe,223.03 release 33.b f Band Management ade	r Tun	blem Encryption insport Tenant emolab stomer Tenant emolab Controller 10.50114: 665	Service reque Gateways 3 - Status Comple	eted	Configurations SI emplate E-3 Registered Up 18/05/2023 29 15:27 11: Last Upda 15/06/2023	D-WAN Settings	Topology Location Sokolniki Pa Moscow, Ce Russia Management IP	More * Moderns Tunnels Multipathing Activation Descrivation Log files State Activated	Update Connection Connected	Actions Delete Set location Deactivate Show password Get Activation URL Unregister CPE Open Console Open WEB Console Open WEB Console Apply configurations Reboot Shutdown Export SD-WAN Con Export Network Sett	Close

L VCPE-3	Registered										😸 🛛 Sav	e Close
Configurati	ion Monitoring Problems Encryption	Service requests	Tags Scripts	SD-WAN s	settings Topology	Network setting	gs BGP setting	IS OSPF	Routing Filters	More *		
Source	Destination	Unsolicited	Thresholds monitoring	MTU ⑦	Errors/second	Utilization (%)	Latency (ms.)	Jitter (ms.)	Packet loss (%)	Speed (MB/sec)	Cost	@ Q ;;
CPE [vGW-11: 8000005	056AA9EA5] :- CPE [vCPE-3: 8000005056/	AAC4FD]: Y	Y	1500	0	0	0	0	0	1000	10000	Management
CPE [vGW-11: 8000005	056AA9EA5] :- CPE [vCPE-3: 8000005056/	AAC4FD]: N	Y	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005	5056AAC4FD] : CPE [vGW-11: 80000050564	A9EA5]:-Y	Υ	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005	5056AAC4FD]: CPE [vGW-11: 80000050564	A9EA5]:- N	Υ	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005	5056AAC4FD]: CPE [vGW-12: 8000005056	AAD2B1]: Y	Υ	1500	0	0	2	0	0	1000	10000	Management
CPE [vCPE-3: 8000005	5056AAC4FD]: CPE [vGW-12: 8000005056	AAD2B1]: N	Y	1500	0	0	1	0	0	1000	10000	Management
CPE [vGW-12: 8000005	5056AAD2B1]: CPE [vCPE-3: 8000005056/	AAC4FD]: Y	Υ	1500	0	0	1	0	0	1000	10000	Management
CPE [vGW-12: 8000005	5056AAD2B1]: CPE [vCPE-3: 8000005056/	AAC4FD]: N	Y	1500	0	0	1	0	0	1000	10000	Management

Нажать Management > Set monitoring thresholds.

Включить:

- Enable tunnel thresholds monitoring
- Enable packet loss monitoring > Critical packet loss level 2%.

Нажать Save for both tunnels – сохранение параметров мониторинга туннелей в оба направления.
Tunnel monitoring thresholds
Enable error monitoring
Critical error level (errors/sec)
1000
Enable utilization monitoring
Critical utilization level (%)
95
Interval for processing latency, jitter, and packet loss (sec) 15
Enable latency monitoring
Critical latency level (ms.)
100
Enable jitter monitoring
Critical jitter level (ms.)
30
Enable packet loss monitoring
Critical packet loss level (%)
2
Close Save for both tunnels Set to default Save
Повторить настройки для всех туннелей. После применения настроек отобразится статистика потерь на туннелях. Значения измеренных параметров, не удовлетворяющих порогам, заданных ранее, будут выделены красным цветом. Т.к. задержка эмулировалась в сторону интерфейс sdwan0(eth0) vCPE-3, то packet loss наблюдается на соответствующих туннелях до

vGW-11 и vGW-12, проходящих через данный интерфейс.

Configuration - Monitoring											Update	Configuration Close
ource	Problems Encryption Service requests	Tags Configurati	ons SD-WAN Settings Topolog	gy Network	Settings BGP Settings	BFD Settings St	tatic Routes VR	RRP UNIS Mod	dems Tunnels Mor	re *		
	Destination	Charged link	Thresholds Monitoring Enabled	. MTU(2)	Error Level, err/sec	Utilization %	Latency, ms	Jitter, ms	Packet Loss %	Speed, Mb/s	Cost	: 80
PE [vGW-11: 8000005056AA9EA5] : 480	0 CPE [vCPE-3: 8000005056AAC4FD]: 480	0 N	Y	1500	0	0	1	0	4	1000	10000	Management
E [vGW-11: 8000005056AA9EA5] : 480	0 CPE [vCPE-3: 8000005056AAC4FD] : 480	n N	Ŷ	1500	0	0	2	0	0	100	10000	Management
E [vCPE-3: 8000005056AAC4FD] : 480	CPE [VGW-11: 80000050568A99EA5] : 480		* 	1500	0	0	3	0	0	1000	10000	Management
E [VCPE-3: 8000005056AAC4FD] : 480	CPE [VGW-11: 8000005056AAVEA5]: 480		Y	1500	0	0	5	0	0	1000	10000	Management
E[vCPE-3: 800000505644C4ED] : 480	CPE (vGW-12: 800000505644D2B1): 480	0 N	Y	1500	0	0	5	0	0	1000	10000	Management
[vGW-12: 8000005056AAD2B1] : 480	0 CPE [vCPE-3: 8000005056AAC4FD] : 480	0 N	Y	1500	0	0	3	0	7.89	1000	10000	Management
E [vGW-12: 8000005056AAD2B1] : 480	0 CPE [vCPE-3: 8000005056AAC4FD]: 480	1 N	Y	1500	0	0	4	0	0	100	10000	Management
.4.5. Включение FEC. Іля туннелей необходимо настроить Forward Error Correction.												
пя туннеле оочередно	й необходим для каждого	іо нас тунн	строить Fo	orwa ать	ard Erro Manage	r Cor	rectio t > S	on. et FE	C/Reo	order	ing.	
ля туннеле оочередно тметить Оч адать Time ажать Save	ей необходим для каждого verride и зада out – 100. e.	ю нас тунн ать FE	строить Fo еля выбр EC ratio 2:	orwa ать 8.	ard Erro Manage	r Cor	rectic t > S	on. et FE	C/Reo	order	ing.	
ля туннеле оочередно тметить О адать Time ажать Save FEC/reorder	ей необходим для каждого verride и зада out – 100. e.	ю нас тунн ать FE	строить Fo еля выбр EC ratio 2:	orwa ать 8.	ard Erro Manage ×	r Cor	rectic t > S	on. et FE	C/Reo	order	ing.	
ля туннеле оочередно тметить Оч адать Time ажать Save FEC/reorder ✓ Override FEC ratio (original/rec	ей необходим для каждого verride и зада out – 100. ∋. ∵ing	іо нас тунн ать FE	строить Fo еля выбр EC ratio 2:	orwa ать 8.	ard Erro Manage	r Cori	rectic t > S	on. et FE	C/Reo	order	ing.	
ля туннеле оочередно тметить Оv адать Time ажать Save FEC/reorder ✓ Override FEC ratio (original/rec 2.8 (high redundanc	ей необходим для каждого verride и зада cout – 100. e. ting	іо нас тунн ать FE	строить Fo еля выбр EC ratio 2:	orwa ать 8.	Ard Erro Manage	r Cor	rectic t > S	on. et FE	C/Reo	order	ing.	
ля туннеле оочередно тметить Оv адать Time ажать Save FEC/reorder ✓ Override FEC ratio (original/rec 2.8 (high redundance Timeout (me) 100	ей необходим для каждого verride и зада cout – 100. e. ting	іо нас тунн ать FE	строить Fo еля выбр EC ratio 2:	orwa ать 8.	Ard Erro Manage	r Cor	rectic t > S	on. et FE	C/Reo	order	ing.	

3.4.6. Проверка работы FEC в статистике ping.

Проверить на хосте wst3, что в статистике ping пропали пропущенные ICMP ответы. В статистике видно, что все ICMP пакеты успешно прошли: по номерам sequence не видно пропусков. Пакеты успешно восстанавливаются с помощью избыточного кодирования.

```
64 bytes from 10.1.1.11: icmp seq=554
                                      ttl=61 time=16.8 ms
64 bytes from 10.1.1.11: icmp seq=555 ttl=61 time=15.6 ms
64 bytes from 10.1.1.11: icmp seg=556 ttl=61 time=73.6 ms
64 bytes from 10.1.1.11: icmp seq=557 ttl=61 time=11.7 ms
64 bytes from 10.1.1.11: icmp seq=558 ttl=61 time=29.8 ms
64 bytes from 10.1.1.11:
                         icmp seq=559 ttl=61 time=27.6 ms
64 bytes from 10.1.1.11: icmp seq=560 ttl=61 time=5.72 ms
64 bytes from 10.1.1.11: icmp_seq=561 ttl=61 time=3.68 ms
64 bytes from 10.1.1.11: icmp seq=562 ttl=61 time=21.8 ms
64 bytes from 10.1.1.11: icmp seq=563 ttl=61 time=19.7 ms
64 bytes from 10.1.1.11: icmp seq=564 ttl=61 time=16.4 ms
64 bytes from 10.1.1.11: icmp seq=565 ttl=61 time=6.86 ms
64 bytes from 10.1.1.11: icmp seq=566 ttl=61 time=12.3 ms
64 bytes from 10.1.1.11: icmp_seq=567 ttl=61 time=10.7 ms
64 bytes from 10.1.1.11: icmp seq=568 ttl=61 time=8.50 ms
64 bytes from 10.1.1.11: icmp seq=569 ttl=61 time=7.38 ms
64 bytes from 10.1.1.11: icmp seq=570 ttl=61 time=5.83 ms
64 bytes from 10.1.1.11: icmp seq=571 ttl=61 time=3.76 ms
64 bytes from 10.1.1.11:
                         icmp_seq=572 ttl=61 time=21.8 ms
64 bytes from 10.1.1.11:
                         icmp_seq=573
                                      ttl=61 time=19.6 ms
64 bytes from 10.1.1.11: icmp seq=574 ttl=61 time=17.8 ms
64 bytes from 10.1.1.11: icmp seq=575 ttl=61 time=75.7 ms
```

3.4.7. Возврат настроек после завершения теста.

Выполнить п. 3.4.4 и выключить мониторинг потерь пакетов для туннелей.

Выполнить п. 3.4.5 и выключить FEC для туннелей.

Остановить ICMP ping на wst3, запущенный в пункте 3.4.1 (возможно прервать с помощью Ctrl+Z).

Выключить эмуляцию задержек и джиттера на хосте isp.

[root@isp]# tc qdisc del dev ens161 root netem [root@isp]# tc qdisc del dev ens193 root netem

3.5. Мониторинг качества туннелей (Jitter, Latency, Packet Loss) и управление трафиком в соответствии с заданным SLA.

Решение SD-WAN позволяет производить измерения параметров прохождения пакетов через туннели (джиттер, задержка, потери пакетов) и изменять пути прохождения трафика в зависимости от заданных параметров, например, чтобы обеспечить минимальную задержку. Измерения параметров туннеля производится с использованием дополнительных полей Туре-Length Value (TLV) внутри заголовков GENEVE.



Рис. 3.5.1 Мониторинг качества туннелей

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help > Включение мониторинга на туннеле:

https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/244988.htm

Ниже рассматривается сценарий с измерением задержки и джиттера на туннелях, заданием ограничений и перенаправление трафика на туннели, которые удовлетворяют ограничениям на задержку и джиттер. Тестовый трафик будет генерироваться между рабочими станциями wst3 и wst4 с использованием iperf, также в статистике iperf будет проверяться статистика джиттера.

Эмуляция задержек и джиттера будет проводиться на хосте isp с помощью системы Linux Traffic Control.

Будут созданы ограничения для транспортного сервиса с целью исключения туннелей, не удовлетворяющих заданным параметрам джиттера и задержек.

Для корректной работы мониторинга задержек все устройства СРЕ и шлюзы должны иметь доступ к NTP серверам и время на устройствах должно быть синхронизировано.



3.5.1. Генерация тестового трафика.

Запустить сервер iperf на хосте wst4:

[root@wst4]# iperf3 -s | grep ms



Запустить клиент iperf на хосте wst3:

[root@wst3]# iperf3 -u -t 6000 -c 10.20.4.11

[ivpa	nin@wst3 ~]\$ i	perf3	-u -t 6000 -	c 10.20.4.11								
Connecting to host 10.20.4.11, port 5201												
[4]	[4] local 10.20.3.11 port 43730 connected to 10.20.4.11 port 5201											
[ID]	Interval		Transfer	Bandwidth	Total Datagrams							
[4]	0.00-1.00	sec	116 KBytes	950 Kbits/sec	82							
[4]	1.00-2.00	sec	129 KBytes	1.05 Mbits/sec	91							
[4]	2.00-3.00	sec	127 KBytes	1.04 Mbits/sec	90							

В случае успешного соединения, в статистике на wst4 появится количество принятых пакетов.

[]	lvpar	nin@wst4 ~]\$	iperf3	-s grep ms	3	
Ι	ID]	Interval		Transfer	Bandwidth	Jitter
[5]	0.00-1.00	sec	116 KBytes	950 Kbits/sec	0.128 ms
[5]	1.00-2.00	sec	129 KBytes	1.05 Mbits/sec	0.133 ms
Ι	5]	2.00-3.00	sec	127 KBytes	1.04 Mbits/sec	0.117 ms
[5]	3.00-4.00	sec	129 KBytes	1.05 Mbits/sec	0.162 ms
[5]	4.00-5.00	sec	127 KBytes	1.04 Mbits/sec	0.141 ms
[5]	5.00-6.00	sec	129 KBytes	1.05 Mbits/sec	0.149 ms
[5]	6.00-7.00	sec	127 KBytes	1.04 Mbits/sec	0.161 ms

3.5.2. Эмуляция задержки и джиттера с помощью ТС.

Для теста необходимо включить эмуляцию задержки и джиттера на сетевом интерфейсе хоста isp, к которому подключен sdwan0 (eth0) интерфейс vCPE-3.

Подключиться к хосту isp и выполнить команду:

[root@isp]# tc qdisc add dev ens193 root netem delay 300ms 100ms

Данная команда создает задержку (delay / latency) в 300ms с разбросом (jitter) в 100ms.

Проверить примененные настройки с помощью следующей команды:

[root@isp]# tc qdisc show

[root@isp ~]#										
[root@isp ~]# tc qdisc add dev ens193 root netem delay 300ms 100ms										
[root@isp ~]# tc qdisc show										
qdisc noqueue 0: dev lo root refcnt 2										
qdisc pfifo_fast 0: dev ens161 root refcnt 2 bands 3 priomap 1 2 2 2 1 2 0 0 1 1 1 1 1 1 1 1										
qdisc pfifo_fast 0: dev ens192 root refcnt 2 bands 3 priomap 1 2 2 2 1 2 0 0 1 1 1 1 1 1 1										
qdisc netem 8001: dev ens193 root refcnt 2 limit 1000 delay 300.0ms 100.0ms										
qdisc pfifo_fast 0: dev ens224 root refcnt 2 bands 3 priomap 1 2 2 2 1 2 0 0 1 1 1 1 1 1 1										
qdisc pfifo_fast 0: dev ens225 root refcnt 2 bands 3 priomap 122212001111111										
qdisc pfifo_fast 0: dev ens256 root refcnt 2 bands 3 priomap 122212001111111										
qdisc pfifo_fast 0: dev ens257 root refcnt 2 bands 3 priomap 122212001111111										
[root@isp ~]#										

3.5.3. Проверка на рабочей станции wst4 наличие джиттера в статистике iperf.

Примечание: по умолчанию режим балансировки per-flow (если он не был изменен на per-packet в 3.1), поэтому поток может пойти через другой интерфейс, и джиттера может не быть.

[5]	379.00-380.00	sec	129 KBytes	1.05 Mbits/sec	0.156 ms	21/91 (23%)
[5]	380.00-381.00	sec	127 KBytes	1.04 Mbits/sec	0.136 ms	8/90 (8.9%)
[5]	381.00-382.00	sec	129 KBytes	1.05 Mbits/sec	0.166 ms	19/91 (21%)
[5]	382.00-383.00	sec	127 KBytes	1.04 Mbits/sec	0.132 ms	26/90 (29%)
[5]	383.00-384.00	sec	129 KBytes	1.05 Mbits/sec	0.147 ms	16/91 (18%)
[5]	384.00-385.00	sec	127 KBytes	1.04 Mbits/sec	0.128 ms	3/90 (8.9%)
[5]	385.00-386.00	sec	86.3 KBytes	706 Kbits/sec	43.065 ms	34/63 (54%)
[5]	386.00-387.00	sec	174 KBytes	1.43 Mbits/sec	32.205 ms	63/95 (66%)
[5]	387.00-388.00	sec	188 KBytes	1.54 Mbits/sec	45.508 ms	50/87 (57%)
[5]	388.00-389.00	sec	160 KBytes	1.31 Mbits/sec	29.382 ms	64/97 (66%)
[5]	389.00-390.00	sec	170 KBytes	1.39 Mbits/sec	39.571 ms	56/87 (64%)
[5]	390.00-391.00	sec	160 KBytes	1.31 Mbits/sec	24.279 ms	57/96 (59%)
[5]	391.00-392.00	sec	163 KBytes	1.33 Mbits/sec	33.819 ms	52/82 (63%)
[5]	392.00-393.00	sec	165 KBytes	1.36 Mbits/sec	44.783 ms	66/97 (68%)
[5]	393.00-394.00	sec	148 KBytes	1.22 Mbits/sec	41.437 ms	55/92 (60%)
[5]	394.00-395.00	sec	129 KBytes	1.05 Mbits/sec	32.055 ms	45/81 (56%)
Γ	51	395.00-396.00	sec	156 KBvtes	1.27 Mbits/sec	40.827 ms	57/94 (61%)

Если в статистике не будет видно задержку, то необходимо на хосте isp применить эмуляцию на другой интерфейс:

[root@isp]# tc qdisc add dev ens161 root netem delay 300ms 100ms

и снять задержку с первого сетевого интерфейса:

[root@isp]# tc qdisc del dev ens193 root



	Registered 3 tion Monitoring Problems Encryption	Service requests	Tags Scripts	SD-WAN	settings Topology	Network settin	gs . BGP setting	IS OSPF	Routing Filters	More *	💥 Sav	e Close
Source	Destination	Unsolicited	Thresholds monitoring	MTU ⑦	Errors/second	Utilization (%)	Latency (ms.)	Jitter (ms.)	Packet loss (%)	Speed (MB/sec)	Cost	\$Q
CPE [vGW-11: 8000005	5056AA9EA5] :- CPE [vCPE-3: 80000050564	AAC4FD]: Y	Y	1500	0	0	0	0	0	1000	10000	Management
CPE [vGW-11: 8000005	5056AA9EA5] :- CPE [vCPE-3: 80000050564	AAC4FD]: N	Υ	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005	5056AAC4FD] : CPE [vGW-11: 8000005056A	A9EA5]:-Y	Υ	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005	5056AAC4FD] : CPE [vGW-11: 8000005056A	A9EA5]:- N	Y	1500	0	0	0	0	0	1000	10000	Management
CPE [vCPE-3: 8000005	5056AAC4FD] : CPE [vGW-12: 8000005056/	AAD2B1]: Y	Y	1500	0	0	2	0	0	1000	10000	Management
CPE [vCPE-3: 8000005	5056AAC4FD] : CPE [vGW-12: 8000005056/	AAD2B1]: N	Y	1500	0	0	1	0	0	1000	10000	Management
CPE [vGW-12: 800000	5056AAD2B1]: CPE [vCPE-3: 8000005056/	AAC4FD]: Y	Y	1500	0	0	1	0	0	1000	10000	Management
CPE [vGW-12: 800000	5056AAD2B1]: CPE [vCPE-3: 80000050564	AAC4FD]: N	Υ	1500	0	0	1	0	0	1000	10000	Management

3.5.6. Включение мониторинга задержек на туннелях, установленных vCPE-3.

Нажать Management > Set monitoring thresholds.

Включить:

- Enable tunnel thresholds monitoring
- Enable latency monitoring > Critical latency level 100 msec.
- Enable jittler monitoring > Critical jitter level 30 msec.

Нажать Save for both links – сохранение параметров мониторинга туннелей в оба направления.

Данные настройки включат мониторинг задержки и джиттера для туннелей и зададут пороговые значения в 30мс и 100мс соответственно. Повторить эти действия для всех туннелей с данным СРЕ устройством.

unnel mon	itoring thresholds	
Critical utilizatio	n level (%)	
95		
Interval for proc	essing latency, jitter, and packet loss (sec)	
Enable late	ncy monitoring	
Critical latency	level (ma.)	
100		
🗹 Enable jitte	r monitoring	
Critical jitter lev	el (ms.)	
30		\$
Enable pac	ket loss monitoring	
Critical packet I	oss level (%)	

3.5.7. После применения настроек в п. 3.5.6 отобразится статистика задержек и джиттера на туннелях. Значения измеренных параметров, не удовлетворяющих порогам, заданных в 3.5.6 будут выделены красным цветом.

>		Registered PE-3								\approx	Update	Configurat	ion Close
	Source	figuration Monitoring Destination :	Charge	Encrypt Thresh Monitc: Enable	MTU	Error Level, : err/sec	s Tag Utiliza1 %	Latenc	Jitter, ms	Packet Loss %;	Speed Mb/s :	Cost :	@ Q ;
-	CPE [vGW-11: 80	0000 CPE [vCPE-3: 80	000C N	Y	1500	0	0	0	0	0	1000	10000	Management
00	CPE [vGW-11: 80	0000 CPE [vCPE-3: 80	000C N	Y	1500	0	0	297	71	0	100	10000	Management
	CPE [VCPE-3: 80	0000C CPE [vGW-11: 80	0000 N	Y	1500	0	0	1	0	0	1000	10000	Management
Ç	CPE [vCPE-3: 80	0000C CPE [vGW-11: 80	0000 N	Y	1500	0	0	1	0	0	1000	10000	Management
5	CPE [VCPE-3: 80	0000C CPE [vGW-12: 80	000C N	Y	1500	0	0	1	0	0	1000	10000	Management
	CPE [vCPE-3: 80	0000C CPE [vGW-12: 80	000C N	Y	1500	0	0	0	0	0	1000	10000	Management
2	CPE [vGW-12: 80	0000C CPE [vCPE-3: 80	000C N	Y	1500	0	0	0	0	0	1000	10000	Management
	CPE [vGW-12: 80	0000C CPE [vCPE-3: 80	000C N	Y	1500	0	0	284	52	0	100	<u>10000</u>	Management



3.5.8. Создание ограничений Constraints.

Для перенаправления трафика необходимо создать ограничения (Constraints). Перейти в меню Infrastructure > SD-WAN контроллер > Management >open configuration menu.

(infrastructure x +												
← → C ▲ Not secure https://10.0.111/infrastructure?controllerID=6527446b8981ea44fcb69584&mode=network												
	Infrastructure			+ Domain + Data center + VIM +	- Controller + Sub							
>>	Resources Q	Network resources Compute resources	System resources IPAM									
	All Domain Data center	Name ~	Transport/service strategy Controller node	es <u>Connection type</u> : <u>Cluster status</u> : <u>Node statuses</u> :	\$ Q							
<u>ا</u>	All resources	SD-WAN Cluster [tenant: 6527d10f8981ea44fcb69576]	Generic VNI swapping 10.11.11.97 (prima transport	ary) Unicast DEGRADED Connected (single)	Management							
O	* demolab.space				Edit Open configuration menu							
0	₽ <u></u>				Reprovision							
ы :=					Download backup file							
					Restore							
83					Delete							
e.					Open properties							

Перейти в меню Constraints, затем открыть вкладку Thresholds и нажать на кнопку +*Threshold Constraint*.

Задать название Constraints в поле name и включить ограничение для задержки (latency) и джиттера (jitter).

Данное ограничение исключит из путей прохождения трафика туннели, не отвечающие настроенным в п. 3.5.6 пороговым значениям.

	Constraints				+	Threshold constraint
» ~	Manual-TE Thresholds	Threshold	constraint		×	
P2P	Name ~	Name Constraint1			Management	1
P2N			Do not use tunnels with this threshold reached	Ignore if no constrained path is found		
M21		Unsolicited				
IP m		Error level				
L3 V		Utilization				
TAP		Latency				
Ser		Jitter	\checkmark			
Con	La construction de la constructi	Packet loss				
Traf						
Inte				Close Create		
Tuni						

3.5.9. Применение ограничений (constraints) к транспортному сервису.

Перейти на вкладку M2M Services. Открыть сервис для редактирования: Management > Edit.

Выбрать созданное в п. 3.5.8 ограничение в секции Constraint. Нажать Next, Next, Save.

	M2M Services								+ Create a new M2M service
>>			Edit M2M Serv	vice			×		
+		,							
P2N			Name						:
M2h	Name	timeout	L2 M2M					Description	©
10121			Constraint		Balancing Mode				
IP M	L2 M2M	300	Threshold 🗸 C	Constaint1 🗸 🗸	Per-flow		~		Management
L3 S									
TAP			mac address learn mode	MAC age timeout	overload action	MAC table size			
Ser\			Learn and Flo 🗸	300	Flood ~	100			
Con			Description						
Filte									
OF i							11		
Link									
Log			Cancel			Next			
SNN									
EN	© 2023 AO "Kasper	sky Lab" support.	(aspersky.com		Version: 2	2.23.03.release.94.	amd64-	SNAPSHOT / 2.2	3.03.release.93.amd64-SNAPSHOT

3.5.10. После применения Constraints контроллер SD-WAN уберет трафик с туннелей, не удовлетворяющий ограничению (Constraint), примененному в 3.5.9.

В статистике iperf на wst4 наглядно видно, что джиттер пропал, потому что SD-WAN контроллер исключил туннели, проходящие через первый WAN интерфейс vCPE-3, для которого была применена эмуляция latency и jitter.

		• • • • P	ore ozor com		TT POLC 0	
	Interval		Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[5]	0.00-1.00	sec	116 KBytes	950 Kbits/sec	0.102 ms	0/82 (0%)
[5]	1.00-2.00	sec	129 KBytes	1.05 Mbits/sec	0.102 ms	0/91 (0%)
[5]	2.00-3.00	sec	127 KBytes	1.04 Mbits/sec	0.109 ms	0/90 (0%)
[5]	3.00-4.00	sec	129 KBytes	1.05 Mbits/sec	0.128 ms	0/91 (0%)
[5]	4.00-5.00	sec	127 KBytes	1.04 Mbits/sec	0.133 ms	0/90 (0%)
[5]	5.00-6.00	sec	129 KBytes	1.05 Mbits/sec	0.110 ms	0/91 (0%)
[5]	6.00-7.00	sec	127 KBytes	1.04 Mbits/sec	0.107 ms	0/90 (0%)
[5]	7.00-8.00	sec	129 KBytes	1.05 Mbits/sec	0.142 ms	0/91 (0%)
[5]	8.00-9.00	sec	127 KBytes	1.04 Mbits/sec	0.120 ms	0/90 (0%)
[5]	9.00-10.00	sec	129 KBytes	1.05 Mbits/sec	0.096 ms	0/91 (0%)
[5]	10.00-11.00	sec	127 KBytes	1.04 Mbits/sec	0.133 ms	0/90 (0%)
[5]	11.00-12.00	sec	129 KBytes	1.05 Mbits/sec	0.134 ms	0/91 (0%)
[5]	12.00-13.00	sec	127 KBytes	1.04 Mbits/sec	0.143 ms	0/90 (0%)
[5]	13.00-14.00	sec	129 KBytes	1.05 Mbits/sec	0.169 ms	0/91 (0%)
[5]	14.00-15.00	sec	127 KBytes	1.04 Mbits/sec	0.167 ms	0/90 (0%)
[5]	15.00-16.00	sec	129 KBytes	1.05 Mbits/sec	0.114 ms	0/91 (0%)
[5]	16.00-17.00	sec	127 KBytes	1.04 Mbits/sec	0.117 ms	0/90 (0%)
[5]	17.00-18.00	sec	129 KBytes	1.05 Mbits/sec	0.092 ms	0/91 (0%)
[5]	18.00-19.00	sec	127 KBytes	1.04 Mbits/sec	0.095 ms	0/90 (0%)
[5]	19.00-20.00	sec	129 KBytes	1.05 Mbits/sec	0.116 ms	0/91 (0%)
[5]	20.00-21.00	sec	127 KBytes	1.04 Mbits/sec	0.128 ms	0/90 (0%)
[5]	21.00-22.00	sec	129 KBytes	1.05 Mbits/sec	0.147 ms	0/91 (0%)
[5]	22.00-23.00	sec	127 KBytes	1.04 Mbits/sec	0.107 ms	0/90 (0%)
[5]	23.00-24.00	sec	129 KBytes	1.05 Mbits/sec	0.133 ms	0/91 (0%)
[5]	24.00-25.00	sec	127 KBytes	1.04 Mbits/sec	0.118 ms	0/90 (0%)
[5]	25.00-26.00	sec	129 KBytes	1.05 Mbits/sec	0.105 ms	0/91 (0%)
[5]	26.00-27.00	sec	129 KBytes	1.05 Mbits/sec	0.091 ms	0/91 (0%)
í 5i	27.00-28.00	sec	127 KBytes	1.04 Mbits/sec	0.171 ms	0/90 (0%)

3.5.11. Возврат настроек после завершения теста.

Снять ограничение с транспортного сервиса, примененного в п. 3.5.9.

Перейти в меню Infrastructure > SD-WAN контроллер > Management > Open configuration menu.

Infra	structure × +			~ - c
← →	C A Not secure https://10.0.1.1	1/infrastructure?controllerID=652/d46b8981ea44fcb69584&mode=network		
	Infrastructure		+ Domain + Data center + VIM +	Controller + Sub
» Ø	Resources Q	(Network resources) Compute resources Bystem resources IPAM		¢ 0
5	All pornain Data center	SD-WAN Cluster [tenant: Generic VNI swapping 10.11.11.97 (primary) 6527d1078981ea44fcb69576) transport	Unicast DEGRADED Connected (single)	Management
0 (5)	* <u>demolab.space</u> 早 <u>DC</u>			Open configuration menu Reprovision
ы				Download backup file
≣				Restore
\bigcirc				Delete
ŝ				Delete
Ľ				Open properties

Перейти на вкладку M2M Services. Открыть сервис L2 M2M для редактирования: Management > Edit. Убрать ограничение в секции Constraint. Нажать Next, Next, Save. + Create a new M2M service M2M Services × \gg Edit M2M Service Name MAC age L2 M2M Name ŝ M21 timeout Constraint Balancing Mode IP M L2 M2M 300 Management Constaint1 Per-flow Threshold L3 S MAC address learn MAC table MAC age timeout MAC table size mode overload action Learn and Flo \sim 300 Flood ~ 100 Description Filte Log Cancel SNN Version: 2.23.03.release.94.amd64-SNAPSHOT / 2.23.03.rel © 2023 AO "Kaspersky Lab" support.kaspersky.com EN Выключить эмуляцию задержек и джиттера на хосте isp. [root@isp]# tc qdisc del dev ens161 root [root@isp]# tc qdisc del dev ens193 root



3.6. Приоритезация трафика с использованием ACL.

Решение SD-WAN позволяет создавать классификаторы трафика на основе полей заголовков IP/TCP/UDP и направлять трафик в определенные транспортные сервисы. Например, возможно создать приоритетный сервис для чувствительного к задержке трафика с ограничениями, чтобы трафик не проходил через туннели с задержкой, не удовлетворяющей заданному ограничению.

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help > Направление трафика приложения в транспортный сервис:

https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/246544.htm

В данном сценарии создается классификатор трафика на основе UDP порта для перенаправления тестового трафика в приоритетный сервис.

Тестовый трафик будет генерироваться между рабочими станциями wst3 и wst4 с использованием iperf на порту UDP 5555. Будет создан L3 ACL для классификации тестового трафика и "ACL интерфейс" для перенаправления трафика отдельный сервис.

В данном сценарии, туннели, проходящие через интерфейс sdwan0 (eth0) vCPE-3 будут отмечены как " Unsolicited " («нежелательный» для использования) и создан отдельный транспортный сервис. Для отдельного сервиса будут заданы ограничения (Constraints), которые исключат туннели, отмеченные как Unsolicited из пути прохождения трафика. Для проверки переключения трафика будет использоваться tcpdump на vCPE-3.

3.6.1. Генерация тестового трафика.

Запустить сервер iperf на хосте wst4 портом 5555:

[root@wst4]# iperf3 -s -p 5555

```
^Ciperf3: interrupt - the server has terminated
[ivpanin@wst4 ~]$ iperf3 -s -p 5555
```

```
Server listening on 5555
```

Запустить клиент iperf на хосте wst3 с портом 5555:

[root@wst3]# iperf3 -u -t 6000 -c 10.20.4.11 -p 5555

ivpanin@wst3 ~]\$ iperf3 -u -t 6000 -c 10.20.4.11 -p 5555 Connecting to host 10.20.4.11, port 5555 [4] local 10.20.3.11 port 41924 connected to 10.20.4.11 port 5555 Interval Total Datagrams ID] Bandwidth 116 KBytes 950 Kbits/sec 1.00-2.00 KBytes 1.05 Mbits/sec sec 129 2.00-3.00 127 KBytes 1.04 Mbits/sec sec

3.6.2. Подключиться к vCPE-3 по SSH и найти через какой интерфейс проходит трафик: *genev_sys_4800* или *genev_sys_4801*:

tcpdump -i genev_sys_4800

genev_sys – туннельные интерфейсы СРЕ. Номер порта указывает на номер WAN интерфейса СРЕ устройства. Номера назначаются по порядку, начиная с порта 4800, по одному на каждый WAN интерфейс. Порт 4800 означает WAN интерфейс sdwan0 (eth0), порт 4801 означает WAN интерфейс sdwan1 (eth1).

В данном примере трафик проходит через интерфейс genev_sys_4800.

root@8000005056A	C4FD:~# tcpdump -i genev sys 4800	
tcpdump: verbose	output suppressed, use -v or -vv for full protocol decode	
listening on gene	/_sys_4800, link-type EN10MB (Ethernet), capture size 262144	bytes
08:31:03.145408	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.145467	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.145491	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.145518	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.145539	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.145564	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.145800	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.145825	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.145849	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245488	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245582	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245608	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245629	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245659	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245928	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245953	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245976	2 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	
08:31:03.245996	? 10.20.3.11.41924 > 10.20.4.11.5555: UDP, length 1448	

3.6.3. Перейти в меню СРЕ и выбрать vCPE-3.

	SD-WAN		+ CPE +	CPE template	+ UNI template	+ SD-WAN instance templat	e + SD-WAN instance pool	+ Firmware + Certificate
» © F	>> 	CPE All © Waiting © Configuration • R All 6 • Connected 6 • Disconnected	Registered o <u>Registering</u>	• Error • Unknown Need update 0	All time Last year	Last month Last week	Last day 14/11/2023 10:41	Z Export to CSV - 14/11/2023 10:41
°°	¢III ¢	DPID : Model ; S	Wiversion : Name :	Role : Status :	State : Connection:	Fragmentation Usage	Transport tenant : Customer te	nant: Registered 🛞 Q.* Actions * :
0	್ಟ್ರೋ	 <u>8000005056A</u> x86_64 VM kit <u>8000005056A</u> x86_64 VM kit 	naas-cpe_2.23.07 <u>vCPE-52</u> naas-cpe_2.23.07 <u>vCPE-51</u>	CPE Registered CPE Registered	Activated Connected Activated Connected	Supported Yes	Demolab Demolab Demolab	07/11/2023 17:43
1.I ≔		• <u>8000005056A</u> x86_64 VM kr	naas-cpe_2.23.07 vCPE-4	CPE Registered	Activated Connected	Supported Yes	Demolab Demolab	07/11/2023 17:43
0	G_1	8000005056AA x86_64 VM kt 8000005056AA x86_64 VM kt	naas-cpe_2.23.07 <u>vGPE-3</u>	Gateway Registered	Activated Connected	Supported Yes	Demolab Demolab Demolab	26/10/2023 16:08
<i>N</i>	ф. 0	• 8000005056A# x86_64VM kt	naas-cpe_2.23.07 <u>vGW-11</u>	Gateway Registered	Activated Connected	Supported Yes	Demolab Demolab	26/10/2023 16:06
	() () ()							
	Ð							
	1							

>		vCPE-3								_	💝 🛛 Upd	late Configuration Close
D	Name	Configuration	Transpor	t Tenant	ervice reques	UNI t	emplate	SD-WAN Setting	Location	Modems	_	Actions
	vCPE-3		Demola	ab	~	0.05	Tamalaka	~	Sokolniki Parl Moscow, Cer	Tunnels		Delete Set location
0	800000	5056AAC4FD	Demola	ab	~	VCF	remplate PE-3	~	Russia	Multipathin	g	Deactivate Show password
•	Descriptio	n								Activation		Get Activation URL Unregister CPE
Ş										Deactivatio	n	Open Console
5										Log files		Apply configurations
5	Device Inf Model	SW Version		Controller	Gateways	User	Registered	Update	Management	State	Connection	Shutdown Export SD-WAN Configurat Export Network Settings
	x86_64 VM	knaas- cpe_2.23.03 release.33 bios.ar	nd64	10.50.114 6653	-	admin	18/05/2023 15:27	29/06/2023 11:14	10.11.12.74	Activated	Connected	
	Out of Bar	nd Management										
>	Tuno				Statue		Loot	Undate		2		

3.6.5. Задание параметра "Unsolicited" для туннелей.

Найти все туннели, через которые проходит трафик: порты источника и назначения туннелей (4800 или 4801) должны совпадать с номером интерфейса согласно проверке в пункте 3.6.2. В результате проверки в данном примере трафик проходит через туннель genev_sys_4800.

Туннели, через которые проходит трафик в примере:

- vCPE-3:4800 <--> vGW-11:4800
- vCPE-3:4800 <--> vGW-12:4800
- vGW-11:4800 <--> vCPE-3:4800
- vGW-12:4800 <--> vCPE-3:4800

Поочередно для каждого найденного туннеля с портом 4800 для vCPE-3 нажать Management > Set tunnel monitoring threshold.

Отметить туннель как " Unsolicited" – означает «нежелательный» для использования.

Нажать Save for both tunnels – сохранение параметров мониторинга туннелей в оба направления.

Configuration Monito	ring Pro	blems Encryption Ser	vice requests	Tags Scr	ipts SD-WAI	N settings T	opology Networ	ksettings BGF	settings OSPF	Routing Fi	ters More *			
irce	. De	estination		Unsolicited	Thresholds monitoring	MTU ⑦	Errors/second	Utilization (9	5) Latency (ms.)	Jitter (ms.) Packet loss (%)	Speed (MB/sec)	Cost	
E [vGW-11: 8000005056AA9EA5]	4800 C	PE [vCPE-3: 8000005056A	AC4FD : 4800		Y	1500	0	0	0	0	0	1000	10000	Ма
E [vGW-11: 8000005056AA9EA5]	4800 CI	PE [vCPE-3: 80000050564	AC4FD : 4801		Y	1500	0	0	0	0	0	1000	10000	Ma
E[vCPE-3: 8000005056AAC4FD	: 4800 CI	PE [vGW-11: 8000005056A	A9EA5]: 4800		Y	1500	0	0	0	0	0	1000	10000	Ma
E [VCPE-3: 8000005056AAC4FD	:4801 CI	PE [vGW-11: 8000005056A	A9EA5]: 4800		Y	1500	0	0	0	0	0	1000	10000	Ma
E [VCPE-3: 8000005056AAC4FD	:4800 CI	PE [vGW-12: 80000050564	AD2B1: : 4800		Y	1500	0	0	2	0	0	1000	10000	Ma
E [vCPE-3: 8000005056AAC4FD	: 4801 CI	PE [vGW-12: 80000050564	AD2B1]: 4800		Y	1500	0	0	1	0	0	1000	10000	Ma
[vGW-12: 8000005056AAD2B1]	:4800 CI	PE [vCPE-3: 80000050564	AC4FD : 4800		Y	1500	0	0	1	0	0	1000	10000	Ma
E [vGW-12: 8000005056AAD2B1]	:4800 CI	PE [VCPE-3: 8000005056A	AC4FD : 4801		Y	1500	0	0	1	0	0	1000	10000	Ma
innel monitoring th	reshol	ds		×										
Innel monitoring th	reshol	ds		×	3									
Innel monitoring th Enable tunnel thresholds monito	reshol	ds		×	2									
Innel monitoring th Enable tunnel thresholds monito Interval for processing errors ar	reshol	ds n rate (sec)		×										
Innel monitoring th Enable tunnel thresholds monito Unsolicited Interval for processing errors ar 60	reshol ring d utilizatio	ds n rate (sec)		×										
Innel monitoring th Enable tunnel thresholds monitor Unsolicited Interval for processing errors ar 60 C Enable error monitoring	reshol ring d utilizatio	ds nrate (sec)		×										
Innel monitoring th Enable tunnel thresholds monito Unsolicited Interval for processing errors ar 60 Interval error monitoring Critical error level (errors/sec)	reshol ring d utilizatio	ds n rate (sec)		×										
Innel monitoring th Enable tunnel thresholds monitor Unsolicited Interval for processing errors ar 60 Critical error monitoring Critical error level (errors/sec) 1000	reshol	ds n rate (sec)		×	2									
Innel monitoring th Enable tunnel thresholds monito Unsolicited Interval for processing errors ar 60 Critical error level (errors/sec) 1000 Enable utilization monitorin	ring d utilizatio	ds n rate (sec)			7									
Innel monitoring th Enable tunnel thresholds monito Unsolicited Interval for processing errors ar 60 Critical error level (errors/sec) 1000 Enable utilization monitorir Critical utilization nevel (%) 55	reshol rring d utilizatio	ds			7									
Innel monitoring th Enable tunnel thresholds monito Unsolicited Interval for processing errors ar 60 Enable error monitoring Critical error level (errors/sec) 1000 Enable utilization monitorir Critical utilization level (%) 95	reshol ring d utilizatio	ds n rate (sec)			2									
Innel monitoring th Enable tunnel thresholds monito Unsolicited Interval for processing errors ar 60 Enable error monitoring Critical error level (errors/sec) 1000 Enable utilization monitorir Critical utilization level (%) 95 Interval for processing latency, 15	ring dutilizatio	ds n rate (sec) acket loss (sec)												
Innel monitoring th Enable tunnel thresholds monito Unsolicited Interval for processing errors ar 60 Enable error monitoring Critical error level (errors/sec) 1000 Enable utilization monitorin Critical utilization level (%) 95 Interval for processing latency, 15 Enable latency monitoring	reshol ring d utilizatio g	ds n rate (sec) acket loss (sec)												

3.6.6. Создание Constraints.

Для перенаправления трафика необходимо создать ограничения. Перейти в меню Infrastructure > SD-WAN контроллер > Management > Open configuration menu.



Numeric Industrial Normanical (Destination, Matter (Destination) Normanical (Destination, Matter (Destination)) Normanical (Destination)) <th>Constraints</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>+ Threshold constraint</th>	Constraints								+ Threshold constraint
Name- Induktion Develokd, Constanter, Mikes/Apole, Mikes/A	Manual-TE Thresholds								
Preshold Constraint Mittador, Mitter, Plecket Loss N N Y N Y Y Management Preshold Constraint & Mittador N N N Y N Y Management Preshold Constraint & Mittador N N N Y Management Preshold Constraint & Mittador N N N N Y Management Preshold Constraint & Mittador N N N N N N N Preshold Constraint & Mittador N N N N N Management Northeast & Mittador N N N N N N Preshold Constraint & Mittador N N N Management Northeast & Mittador N N N N N Northeast & Mittador N N N Management Northeast & Mittador N N N Northeast & Mittador N N N Northeast & Mittador N N Northeast & Mittador N N	Name ~	Unsolicited	Error level	Utilization	Latency	¹ Jitter	Packet loss	Management	
Trendoid, Contrart, Utilization N Trendoid, Contrart, Little, Packet, Loss N Trendoid, Contrart, Error, Leel N Management N Uncotenet, Societation, Little, Packet, Loss N Trendoid, Contrart, Error, Leel N Management N Uncotenet, Societation, Little, Packet, Loss N Uncotenet, Societa	Threshold_Constraint_Utilization_Jitter_Packet_Loss	N	N	Y	N	Y	Y	Management	
Trenhold_Constant_Liktory N Trenhold_Constant_Attor Packet Loss N Constant Image: Constant of path is found Unackoded Image: Constant of pa	Threshold_Constraint_Utilization	N	Threshold o	onstraint			× N	Management	
Threehold, Constraint, Error, Level N Description: Description: <td>Threshold_Constraint_Latency</td> <td>N</td> <td></td> <td></td> <td></td> <td></td> <td>N</td> <td>Management</td> <td></td>	Threshold_Constraint_Latency	N					N	Management	
Threehold_Constraint_Error_Level N Uncolumn to month with Historhould of reached Uncolumn to m	Threshold_Constraint_Jitter_Packet_Loss	N	Name Constraint1				Y	Management	
Undolotted Irror level Utilization Utilizatio Utilization Utilization Utilization Utilization Utiliz	Threshold_Constraint_Error_Level	N	_	Do not use tunnels with this	threshold reached	Ignore if no constrained path is found	N	Management	
Laformed Utilization Utilizatio Utilization Utilization Utilization Utilization Utilizatio			Unsolicited	✓					
Latercy Jater Jater Pecket loss			Utilization						
Jitter Packet loss			Latency						
Padet los Core Core Core			Jitter						
Cose			Packet loss						
Cisse									
Close									
Close									
						Close Create			

3.6.7. Создание правил фильтрации.

Для направления трафика в отдельный сервис нужно создать список доступа ACL, чтобы поймать тестовый трафик UDP с портом 5555.

and in traine qual				
Traffic filters				+ Traffic qualification ru
Traffic filters Traffic qualification rules				
Name	: L2 fields	: L3 fields	: L4fields	: @
DPI-SSH	-	Protocol = IPv4 PKT mark = 227	-	Management
DPI-HTTO		Protocol = IPv4 PKT mark = 105		Management
Отметить воОтметить во	вкладке L3 Fie вкладке L4 Fie	elds: Protocol – IPv4. elds:		
 Отметить во Отметить во IP protocol – Destination режать Create. 	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds:	×	
 Отметить во Отметить во IP protocol – Destination рожать Create. 	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds:	×	
 Отметить во Отметить во IP protocol – Destination рожать Create. Traffic qualificat Name UDP-5555	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds:	×	
 Отметить во Отметить во IP protocol – Destination рожать Create. Traffic qualificat Name UDP-5555 L2 fields L3 fields (L4 fields) 	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds:	×	
 Отметить во Отметить во IP protocol – Destination рожать Create. Traffic qualificat Name UDP-5555 L2 fields L3 fields (L4 fields) IP Protocol 	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds: v	×	
 Отметить во Отметить во IP protocol – Destination рожать Create. Traffic qualificat Name UDP-5555 L2 fields L3 fields L2 fields L3 fields Source port list	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds:	×	
 Отметить во Отметить во IP protocol – Destination рожать Create. Traffic qualificat Name UDP-5555 L2 fields L3 fields (L4 fill) IP Protocol Source port list Destination port list	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds:	×	
 Отметить во Отметить во IP protocol – Destination рожать Create. Traffic qualificat Name UDP-5555 L2 fields L3 fields L4 fields IP Protocol Source port list Ø Destination port list ICMP type number	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds: v		
 Отметить во Отметить во IP protocol – Destination proжать Create. Traffic qualificat Name UDP-5555 L2 fields L3 fields (L4 fill) ✓ IP Protocol Source port list ✓ Destination port list ICMP type number	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds:		
 Отметить во Отметить во IP protocol – Destination рожать Create. Traffic qualificat Name UDP-5555 L2 fields L3 fields L4 fi IP Protocol Source port list Ø Destination port list ICMP type number	вкладке L3 Fie вкладке L4 Fie UDP. ort -5555. ion rule	elds: Protocol – IPv4. elds:	×	



3.6.8. Создание фильтра. Перейти на вкладку Traffic filters, нажать + Traffic filter. Traffic filter Traffic filters Traffic filters Traffic qualification rules Name Added rules Action 1 DPI-SSH DPI-HTTO Default action Permit Permit Permit DPI-FILTER Management Задать имя фильтра. • Добавить правила, созданные в п. 3.6.7. Выбрать в селекторе Rule созданное • 3.6.7. правило, задать Action – Permit. Нажать Add. нажать Create. \times New Traffic filter Name UDP-5555 Sequence Traffic qualification rule Action 20 Permit Add 10, UDP-5555, Permit Delete Default action (if sequence=999) Permit Close



3.6.9. Создание ACL Service interfaces.

Трафик попадает в транспортный сервис через сервисные интерфейсы. Необходимо создать специальный ACL интерфейс (ACL Service Interface – ACL SI). Перейти на вкладку Service Interfaces, затем выбрать Switch vCPE-3 и Port 2 (ovs-lan).

Нажать Create service interface. Выбрать:

- Type: ACL.
- Service interface: vCPE-3 (port 2). Traffic Filter с UDP 5555, созданный в пункте 3.6.8.
- Sequence "Match order 1" (данный ACL SI будет с первым обрабатывать трафик).

Нажать Create.

Service interfaces						
Switch CPE [vCPE-3: 8000 ~	Port 2 (ovs-lan) ~	Create service Interfa	ce			0
Туре	E Description	: VLAN	i Inner VLAN	: Filter	: Name	: @
Access		0	Service interface		X SI://CPE [vCPE-3: 8000005056AAC4	FD]/p:2 Management
			Туре	Service interface		
			ACL ~	CPE [vCPE-3: 8000005056r/		
			Traffic fliter	Sequence		
			UDP-5555 V	Match order 1 V		
			Description			
				h		
			Close	Create		

3.6.10. Для создания сервиса требуется создать сервисные интерфейсы для каждой СРЕ.

Повторить п.3.6.9 для vCPE-4.

3.6.11. Создание отдельного транспортного сервиса для приоритетного трафика. Перейти в M2M Service, нажать +Create a new M2M service.

Задать название, выбрать созданный ранее Threshold (в пункте 3.6.6), нажать Next.

WIZIVI_ACL						
Constraint				Balancing mode		
Threshold V	Const	raint1	\sim	Per-flow		
MAC learn mode		MAC age timeout (sec)		MAC table overload action		MAC table size
Learn and flood	~	300		Flood	~	100
Description						

Добавить 2 сервисных интерфейса (для vCPE-3 и vCPE-4) для направления трафика в сервис:

- выбрать Switch (vCPE3 и vCPE4)
- Port созданные в п.3.6.9 и 3.6.10 ACL SI
- Qos Unlimited-QoS
- Нажать на +Add

Нажать Next и Create.

Switch		Port		
CPE [vCPE-4: 8000005056AA35FF]	\sim			\sim
Show used service interfaces				
QoS		Inbound filter		
Unlimited-QoS	\sim			\sim
Use backup service interface				
🕂 Add				
+ Add Service interface: CPE [vCPE-3: 8000005056AAC4FD], A	CL: Port 2, VLAN I) 0 Filter: UDP-5555 / Match order 1, QoS: (Jnlimited-QoS	Delete
+ Add Service interface: CPE [vCPE-3: 8000005056AAC4FD], A Service interface: CPE [vCPE-4: 8000005056AA35FF], A	CL: Port 2, VLAN I CL: Port 2, VLAN II	0 0 Filter: UDP-5555 / Match order 1, QoS: U 0 0 Filter: UDP-5555 / Match order 1, QoS: U	Jnlimited-QoS Inlimited-QoS	Delete Delete

3.6.12. Подключиться к vCPE-3 и проверить, что трафик переключился на другой WAN интерфейс (в зависимости от настроек, сделанных ранее):

В пункте 3.6.2 проверялось, что трафик идёт через интерфейс genev_sys_4800 (sdwan0). После настройки отдельного транспортного сервиса в результате работы ограничений и фильтра трафик перешел на интерфейс genev_sys_4801 (sdwan1).

Проверить с помощью tcpdump наличие трафика на интерфейсе geneve_sys_4801. *# tcpdump -i genev_sys_4801*

На скриншоте видно, что трафик переключился с интерфейса genev_sys_4800 (sdwan0) на genev_sys_4801 (sdwan1).

root@8000005056AAC4FD:~# tcpdump -i genev sys 4801	
tcpdump: verbose output suppressed, use -v or -vv for f	ull protocol decode
listening on genev sys 4801, link-type EN10MB (Ethernet	.), capture size 262144 bytes
08:54:33.012984 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.013061 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.013631 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.013665 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.013689 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.013710 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.013730 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.013750 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.013770 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.112997 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.113067 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.113529 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.113566 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.113591 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.113617 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.113638 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.113668 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.113691 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.214098 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.214651 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.214700 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.214724 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.214751 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.214776 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.214803 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448
08:54:33.214832 IP 10.20.3.11.53775 > 10.20.4.11.5555:	UDP, length 1448



3.6.13. Возврат настроек после завершения теста.

Удалить сервис, созданный в п. 3.6.11 (при удалении отметить Delete associated service interfaces).

Убрать параметр "Unsolicited" с туннелей, добавленный в п. 3.6.5.

Остановить iperf, запущенный в п. 3.6.1.



3.7. Приоритезация трафика с использованием DPI.

Решение SD-WAN позволяет создавать классификаторы трафика с помощью DPI и перенаправлять трафик для определенных приложений.

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help > Направление трафика приложения в транспортный сервис:

https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/246544.htm

В данном сценарии создается классификатор для SSH и HTTP трафика для перенаправления в приоритетный сервис. Тестовый трафик будет генерироваться между рабочими станциями wst3 до wst4 с использованием ssh, nc и curl. Будет создан DPI правило для классификации тестового трафика и ACL интерфейс для перенаправления трафика в отдельный сервис. Туннели, проходящие через интерфейс sdwan0 (eth0) vCPE-3 будут отмечены как Unsolicited, также будет создан отдельный транспортный сервис, для которого будут заданы ограничения (Constraints), которые исключат Unsolicited туннели из пути прохождения трафика. Для проверки переключения трафика будет использоваться tcpdump на vCPE-3.

3.7.1. Для теста необходимо запустить сессию SSH на хосте wst3 до wst4:

[root@wst3]# ssh root@10.20.4.11

[ivpanin@wst3 ~]\$ ssh root@10.20.4.11 root@10.20.4.11's password: Last login: Mon Jun 26 16:32:13 2023 from 10.20.3.11 [root@wst4 ~]#

3.7.2. Подключиться к vCPE-3 и проверить, что трафик идет через один из интерфейсов genev_sys_4800 или genev_sys_4801:

tcpdump -i genev_sys_4800

genev_sys – туннельные интерфейсы СРЕ. Номер порта указывает на номер WAN интерфейса СРЕ устройства. Номера назначаются по порядку, начиная с порта 4800, по одному на каждый WAN интерфейс. Порт 4800 означает WAN интерфейс sdwan0 (eth0), порт 4801 означает WAN интерфейс sdwan1 (eth1).

Запомнить на каком из интерфейсов сейчас идет тестовой трафик, для SSH сессии он может быть ассиметричным (в одну сторону через 4800, а в другую через 4801). В примере SSH идет через *genev_sys_4800 (sdwan0).*

root@8000005056AAC4FD:~# tcpdump -i genev_sys_4800 grep 4.11
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on genev_sys_4800, link-type EN10MB (Ethernet), capture size 262144 bytes
13:39:15.283859 IP 10.20.4.11 > 10.20.3.11: ICMP echo request, id 5153, seq 29978, length 64
13:39:15.284559 IP 10.20.3.11 > 10.20.4.11: ICMP echo reply, id 5153, seq 29978, length 64
13:39:16.285837 IP 10.20.4.11 > 10.20.3.11: ICMP echo request, id 5153, seq 29979, length 64
13:39:16.286389 IP 10.20.3.11 > 10.20.4.11: ICMP echo reply, id 5153, seq 29979, length 64
13:39:17.287721 IP 10.20.4.11 > 10.20.3.11: ICMP echo request, id 5153, seg 29980, length 64
13:39:17.288264 IP 10.20.3.11 > 10.20.4.11: ICMP echo reply, id 5153, seq 29980, length 64
13:39:18.289822 IP 10.20.4.11 > 10.20.3.11: ICMP echo request, id 5153, seq 29981, length 64
13:39:18.290502 IP 10.20.3.11 > 10.20.4.11: ICMP echo reply, id 5153, seq 29981, length 64
13:39:19.291081 IP 10.20.4.11 > 10.20.3.11: ICMP echo request, id 5153, seg 29982, length 64
13:39:19.291723 IP 10.20.3.11 > 10.20.4.11: ICMP echo reply, id 5153, seq 29982, length 64
13:39:20.292795 IP 10.20.4.11 > 10.20.3.11: ICMP echo request, id 5153, seg 29983, length 64
13:39:20.293434 IP 10.20.3.11 > 10.20.4.11: ICMP echo reply, id 5153, seq 29983, length 64
13:39:20.680213 IP 10.20.3.11.56790 > 10.20.4.11.ssh: Flags [P.], seq 619880975:619881011, ack 1077224629, win 291, options [nop,nop,TS val 235266084 ecr 235]
218972], length 36
13:39:20.684756 IP 10.20.4.11 ssh > 10.20.3.11.56790: Flags [P.], seg 1:37, ack 36, win 295, options [nop,nop,TS val 235309077 ecr 235266084], length 36
13:39:20.685333 IP 10.20.3.11.56790 > 10.20.4.11.ssh: Flags [.], ack 37, win 291, options [nop,nop,TS val 235266090 ecr 235309077], length 0
13:39:20.811386 IP 10.20.3.11.56790 > 10.20.4.11.ssh: Flags [P.], seq 36:72, ack 37, win 291, options [nop,nop,TS val 235266216 ecr 235309077], length 36
13:39:20.814117 IP 10.20.4.11.ssh > 10.20.3.11.56790: Flags [P.], seq 37:73, ack 72, win 295, options [nop,nop,TS val 235309207 ecr 235266216], length 36
13:39:20.814651 IP 10.20.3.11.56790 > 10.20.4.11.ssh: Flags [.], ack 73, win 291, options [nop,nop,TS val 235266219 ecr 235309207], length 0
13:39:20.884017 IP 10.20.3.11.56790 > 10.20.4.11.ssh: Flags [P.], seq 72:108, ack 73, win 291, options [nop,nop,TS val 235266288 ecr 235309207], length 36
13:39:20.886770 IP 10.20.4.11.ssh > 10.20.3.11.56790: Flags [P.], seq 73:109, ack 108, win 295, options [nop,nop,TS val 235309280 ecr 235266288], length 36
13:39:20.887343 IP 10.20.3.11.56790 > 10.20.4.11.ssh: Flags [.], ack 109, win 291, options [nop,nop,TS val 235266292 ecr 235309280], length 0
13:39:21.085620 IP 10.20.3.11.56790 > 10.20.4.11.ssh: Flags [P.], seg 108:144, ack 109, win 291, options [nop,nop,TS val 235266490 ecr 235309280], length 36
13:39:21.088901 IP 10.20.4.11.ssh > 10.20.3.11.56790: Flags [P.], seg 109:185, ack 144, win 295, options [nop,nop,TS val 235309482 ecr 235266490], length 76
13:39:21.089380 IP 10.20.3.11 56790 > 10.20.4.11.ssh: Flags [.], ack 185, win 291, options [nop, nop, TS val 235266494 ecr 235309482], length 0
13:39:21.294580 IP 10.20.4.11 > 10.20.3.11: ICMP echo request, id 5153, seg 29984, length 64
13:39:21.295229 IP 10.20.3.11 > 10.20.4.11: ICMP echo reply, id 5153, seq 29984, length 64
13:39:21.504411 IF 10.0.1.11.36582 > 10.11.12.74.zabbix-agent: Flags [.], ack 2143178383, win 502, options [nop,nop,TS val 4169110840 ecr 3932987910], length
0

3.7.3. Перейти в меню СРЕ и выбрать vCPE-3.

۲	SD-WAN	+ CPE + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + Firmware + Certificate
> C F &	×	CPE All © Waiting © Configuration • Registered © Registering • Error • Unknown All time Lastyear Lastmonth Lastweek Lastday 14/11/2023 10.41 - 14/11/2023 10.41 All 6 • Connected 6 • Disconnected 0 • Connection error 0 Need update 0
ja 88 O III E ⊙⊙	ၪႍႋႜၟၟႍႍၟႍၟႍၟႍၟႍၟႍၟၟၣႍၯႝၘၟႍၟႍၮၟႍၟႍၟႍၟႍ	DPID Model SW version Name Role Status Status Status Status Connection Fragmentation Usage Transport tenant; Customer tenant; Registered Q * Actions * 8000005056A4 x86_64VM knass-cpe_223.07 vCPE-52 CPE Registered Activated Connected Supported Yes Demolab 07/11/202317:43 8000005056A4 x86_64VM knass-cpe_223.07 vCPE-4 CPE Registered Activated Connected Supported Yes Demolab 07/11/202317:43 8000005056A4 x86_64VM knass-cpe_223.07 vCPE-4 CPE Registered Activated Connected Supported Yes Demolab 07/11/202317:43 8000005056A4 x86_64VM knass-cpe_223.07 vCPE-3 CPE Registered Activated Connected Supported Yes Demolab 07/11/202317:43 8000005056A4 x86_64VM knass-cpe_223.07 vCM-12 Gateway Registered Activated Connected Supported Yes Demolab 06/10/202316:08 80000005056A4 x86_64VM knass-cpe_223.07 vGM-11



3.7.5. Задание параметра " Unsolicited " для туннелей.

Найти все туннели, через которые проходит трафик: порты источника и назначения туннелей (4800 или 4801) должны совпадать с номером интерфейса согласно проверке в пункте 3.7.2. В результате проверки в данном примере трафик проходит через туннель genev_sys_4800.

Туннели, через которые проходит трафик в примере:

- vCPE-3:4800 <--> vGW-11:4800
- vCPE-3:4800 <--> vGW-12:4800
- vGW-11:4800 <--> vCPE-3:4800
- vGW-12:4800 <--> vCPE-3:4800

Поочередно для каждого найденного туннеля с портом 4800 для vCPE-3 нажать Management > Set tunnel monitoring threshold.

Отметить туннель как " Unsolicited" – означает «нежелательный» для использования.

Нажать Save for both tunnels – сохранение параметров мониторинга туннелей в оба направления.

Configuration Monitoring	Problems Encryption Service re-	quests	Tags Scripts	SD-WAN settings	Topology	Network settings B	GP settings OSPF	Routing F	ilters More *			
urce	Destination	1	Unsolicited Th	esholds MTU	② Errors	second Utilization	n (%) Latency (ms.) Jitter (ms	.) Packet loss (%)	Speed (MB/sec)	Cost	
E [vGW-11: 8000005056AA9EA5 : 480	0 CPE [vCPE-3: 8000005056AAC4FE	D]:4800	Y Y	1500	0	0	0	0	0	1000	10000	М
E [vGW-11: 8000005056AA9EA5] : 480	0 CPE [vCPE-3: 8000005056AAC4FE	0]:4801	N Y	1500	0	0	0	0	0	1000	10000	М
E [VCPE-3: 8000005056AAC4FD] : 480	0 CPE [vGW-11: 8000005056AA9EA5	5 : 4800	Y Y	1500	0	0	0	0	0	1000	10000	М
E [VCPE-3: 8000005056AAC4FE] : 480	1 CPE [vGW-11: 8000005056AA9EA5	5 : 4800	N Y	1500	0	0	0	0	0	1000	10000	М
E [VCPE-3: 8000005056AAC4FE] : 480	0 CPE [vGW-12: 8000005056AAD2B1	1 : 4800	Y Y	1500	0	0	2	0	0	1000	10000	М
re [vcpe-3: 8000005056AAC4FE] : 480	1 CPE [vGW-12: 8000005056AAD2B1	1:4800	N Y	1500	0	0	1	0	0	1000	10000	М
E [vGW-12: 8000005056AAD2B1 : 480	0 CPE [vCPE-3: 8000005056AAC4FE	D]:4800	Y Y	1500	0	0	1	0	0	1000	10000	М
E [vGW-12: 8000005056AAD2B1 : 480	0 CPE [vCPE-3: 8000005056AAC4FE	c]:4801	N Y	1500	0	0	1	0	0	1000	10000	м
unnel monitoring thres	holds		×									
unnel monitoring thres	holds		× .									
unnel monitoring thres Enable tunnel thresholds monitoring	holds											
Innel monitoring thres Enable tunnel thresholds monitoring Unsolicited Interval for processing errors and util	holds zation rate (sec)		×									
Enable tunnel thresholds monitoring	holds zation rate (sec)		×									
Enable tunnel thresholds monitoring	holds zation rate (sec)		×									
Enable tunnel thresholds monitoring Enable tunnel thresholds monitoring Unsolicited Interval for processing errors and util 60 Enable error monitoring Critical error level (errors/sec)	holds zation rate (sec)		×									
Enable tunnel thresholds monitoring Enable tunnel thresholds monitoring Unsolicited Interval for processing errors and util 60 Enable error monitoring Critical error ievel (errors/sec) 1000	holds zation rate (sec)		×									
Enable tunnel thresholds monitoring Enable tunnel thresholds monitoring Unsolicited Interval for processing errors and util o Enable error monitoring Critical error level (errors/sec) T000 Enable utilization monitoring	holds zation rate (sec)											
Enable tunnel thresholds monitoring Enable tunnel thresholds monitoring Unsolicited Interval for processing errors and util GO Enable error monitoring Critical error level (errors/sec) 1000 Enable utilization monitoring Critical utilization monitoring Critical utilization monitoring Critical utilization level (%) re	holds zation rate (sec)		×									
Enable tunnel thresholds monitoring Enable tunnel thresholds monitoring Unsolicited Interval for processing errors and util 60 Enable error monitoring Critical error level (errors/sec) 1000 Enable utilization monitoring Critical utilization monitoring Critical utilization level (%) 95	holds zation rate (sec)											
Enable tunnel thresholds monitoring Enable tunnel thresholds monitoring Unsolicited Interval for processing errors and util 60 Enable error monitoring Critical error level (errors/sec) 1000 Enable utilization monitoring Critical utilization monitoring Critical utilization monitoring Critical utilization level (%) 95 Interval for processing latency, jitter,	holds zation rate (sec)											
Enable tunnel thresholds monitoring Enable tunnel thresholds monitoring Unsolicited Interval for processing errors and util 60 Enable error monitoring Critical error level (errors/sec) 1000 Enable utilization monitoring Critical utilization monitoring Critical utilization ievel (%) 95 Interval for processing latency, jitter, 15	holds zation rate (sec)											



3.7.6. Создание Constraints.

Для перенаправления трафика необходимо создать ограничения. Для этого нужно перейти в меню *Infrastructure > SD-WAN контроллер > Management > Open configuration menu*.

← → C ▲ Not secure https://10.0.1.1	l/infrastructure?controllerID=6527d46b89	81ea44fcb69584&mode=network				९ 🖻 🛧 🗖
(infrastructure				+ Domain +	Data center + VIM +	- Controller + Sub
Resources Q All Domain Data center	Network resources Compute resources Name >	System resources IPAM Transport/service strategy : Generic VNI swapping	Controller nodes 10.11.11.97 (primary)	: Connection type Unicast	Cluster status Node statuses DEGRADED Connected (single)	 Q Management
	6527d10f8981ea44fcb69576]	transport				Edit Open configuration menu Reprovision
ul ≔						Download backup file
0						Restore
පී ද						Open properties
Перейти в меню (Constraints/ зат	ем отрыть в	зкладку Th	resholds <i>v</i>	і нажать на кно	опку

+Threshold Constraint.

Задать название Constraints в поле name и включить ограничение Unsolicited Данное ограничение исключит из транспортного сервиса туннели, отмеченные как Unsolicited. Нажать Save.

Manual-TE Threeholds	nsolicited ¹ Er								
Name - U	nsolicited Er								
		rrortevel	Utilization	Latency	1 Jitter	^E p	acket loss ^I M	lanagement	
Threshold_Constraint_Utilization_Jitter_Packet_Loss N	N		Y	N	Y	Y		Management	
Threshold_Constraint_Utilization N	Th	reshold const	traint			× N	•	Management	
Threshold_Constraint_Latency N						N	·	Management	
Threshold_Constraint_Jitter_Packet_Loss N	Cor	æ nstraint1				Y		Management	
Threshold_Constraint_Error_Level N		Do.not	t use tunnels with this thresho	ld reached	Ignore if no constrained path is found	N	۱ 	Management	
		Insolicited 🗹							
	E	trilization							
		atency							
	Ji	itter							
	P	acket loss							
					Close Create				



3.7.7. Создание правил фильтрации DPI.

Перейти в меню Traffic filters. Затем перейти во вкладку Traffic qualification rules. Нажать +*Traffic qualification rule*.

Задать имя правила, отметить во вкладке L3 Fields Protocol – IPv4, во DPI Application - SSH, и нажать Create.

Traffic filters					+ Traffic qualification rule
Traffic filters Traffic qualification rules					
Name : L2 DPI-SSH -	Traffic qualification rul	e	>	(;	(8)
DPI-HTTO -	Name DPI-SSH				Management
UDP-5555 -	L2 fields L3 fields L4 fields DPI) Fach vi		JDP ort list = 5555	Management
	PKT mark	227			
	Close		Smo		
	Close		Save		

Для HTTP трафика аналогично задать имя правила, отметить во вкладке L3 Fields Protocol – IPv4, во DPI Application - http, и нажать Create.

iffic filters						+ Traffic qualification rule
Traffic filters Traffic qualification rule	25					
Name	: L2	Traffic qualification ru	le	×		:
Dri-53m		Name				Management
DPI-HTTO		DPI-HTTp				Management
UDP-5555		L2 fields L3 fields L4 fields [PI		JDP ort list = 5555	Management
		Application	http 🗸			
		PKT mark	105			
		Close		Save		



3.7.8. Создание фильтра.

Далее необходимо создать фильтр, куда добавятся созданные ранее правила. Перейти на вкладку Traffic filters, нажать +*Traffic Filter*.

	Traffic filters			+ Traffic filter
»	Traffic filters	ules		
Con	Name	: Added rules	: Action	i @
Swit	DPI-FILTER	DPI-SSH DPI-HTTP Default action	Permit Permit Permit	Management
Top	UDP-5555	UDP-5555 Default action	Permit Permit	Management
QoS				
P2P				
P2N				
M2N IPm				
L3 V				
TAP				
Sen				
Con				
Inte				
Tuni				
Law				

- Задать имя,
- Добавить правила, созданные в п.3.7.7. Выбрать в селекторе Rule созданное п. 3.7.7 правило для SSH, Action – Permit. Нажать Add. Повторить для правила HTTP.
- нажать Create.

Traffic filters		+ Traffic filter
Traffic filters Traffic qualification rules		
Name	Traffic filter ×	0
DPI-FILTER	Name	Management
UDP-5555	DPI-FILTER Sequence Traffic qualification rule Action	Management
	\$p I≑ ✓ Permit ✓	
	Add 10, DPI-SSH, Permit Delete	
	20, DPI-HTTP, Permit Delete	
	Permit	
	Close	



3.7.9. Создание ACL Service interfaces.

Трафик попадает в транспортный сервис через сервисные интерфейсы. Необходимо создать специальный ACL интерфейс (ACL Service Interfaces – ACL SI). Перейти на вкладку Service Interfaces, затем выбрать Switch vCPE-3 и Port 2 (ovs-lan).

Нажать Create service interface. Выбрать:

- Type: ACL.
- Service interface: vCPE-3.
- Traffic filter: DPI-Filter, созданный в пункте0.
- Sequence "Match order 1" (данный ACL SI будет с высшим приоритетом).

Нажать Save.

Повторить для vCPE-4.

Service interfaces				
Switch Port CPE [vCPE-3: 800(Y All Y Create service inte	rface			o
Port : Type : Description	Service interface	×	Name Si://CPE [vCPE-3: 8000005056AAC4FD]/p:1	() Management
2 Access	Port 2 (ovs-lan)		SI://CPE [vCPE-3: 80000050566AAC4FD]/p:2	Management
	Type Ser ACL V C	rvice interface CPE [vCPE-3: 8000005056+/		
	Traffic fliter Sec DPI-FILTER V M	quence Natch order 1 V		
	Description			
	Close	Create		

3.7.10. Для создания транспортного сервиса требуется создать ACL сервисные интерфейсы для каждой СРЕ. Повторить п.3.6.9 для vCPE-4.

3.7.11. Создание отдельного транспортного сервиса.

Перейти в M2M services. Нажать +M2M service.

Задать название, выбрать созданный paнee Threshold (в пункте 3.6.6), нажать Next.

	>	C All Up Down Deg	raded						
ame	MAC age	New M2M servic	e	i.	i		Ţ.	;	× ption ®
M2M	300	Name							Management
		M2M_ACLS							
		Constraint			Balancing mode				
		Threshold ~	✓ Constraint1		Per-flow			~	
		MAC learn mode		MAC age timeout (sec)	MAC table overload action		MAC table size		
		Learn and flood	~	300	Flood ~		100		
		Description							
								4	
		Cancel					Next		

Добавить 2 сервисных интерфейса для направления трафика в сервис:

- выбрать Switch (vCPE3 и vCPE4)
- Port созданные в п. 3.7.9 и 3.7.10 ACL SI
- Qos Unlimited-QoS
- Нажать на +Add

Нажать Next и Save.

M2M services +					
	×	All Up Down Degraded			
Name	: MAC age	New M2M service	1	: × ¹ ption	•
L2 M2M	300	Service endpoints Switch CPE [vCPE-4: 8000005056AA35FF] Show used service interfaces QoS Unlimited-QoS Use backup service interface	Port Inbound filter	~	Management
		+ Add Service interface: CPE [vCPE-3: 8000005056AAC4FD], ACL: Port 2, VLAN Service interface: CPE [vCPE-4: 8000005056AA35FF], ACL: Port 2, VLAN Cancel	D O Filter: DPI-FILTER / Match order 1, QoS: Unlimited-QoS D O Filter: DPI-FILTER / Match order 1, QoS: Unlimited-QoS Back	Delete Delete Next	

3.7.12. Подключиться к vCPE-3 и проверить, что трафик переключился на другой WAN интерфейс.



В пункте 3.7.2 проверялось, что трафик идёт через интерфейс genev_sys_4800 (sdwan0). После настройки отдельного транспортного сервиса, в результате работы ограничений и фильтра, трафик переключился на интерфейс genev_sys_4801 (sdwan1).

Проверить с помощью tcpdump наличие трафика на интерфейсе geneve_sys_4801.

tcpdump -i genev_sys_4801

На скриншоте видно, что трафик переключился с интерфейса genev_sys_4800 (sdwan0) на genev_sys_4801 (sdwan1).

root0800000556AAC4FD:~0 tcpdump -i genev sys_4001 grep 4.11
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on genev sys 4801, link-type EN10MB (Ethernet), capture size 262144 bytes
13:52:39.372158 IP 10.0.1.11.55852 > 10.11.12.74.zabbix-agent: Flags [.], ack 4211203237, win 502, options [nop, nop, TS val 4169908707 ecr 3933785779], length
13:52:43.519522 IP 10.11.12.74.zabbix-agent > 10.0.1.11.55960: Flags [S.], seg 2485543234, ack 1001346115, win 65160, options [mss 1460, sackOK,TS val 3933789
928 ecr 4169912855,nop,wscale 7], length 0
13:52:50.485712 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [P.], seq 156476863:156476899, ack 1133284983, win 291, options [nop,nop,TS val 236075890 ecr 236
082390], length 36
13:52:50.489356 IP 10.20.4.11.ssh > 10.20.3.11.56792: Flags [P.], seg 1:37, ack 36, win 295, options [nop,nop,TS val 236118882 ecr 236075890], length 36
13:52:50.490000 IF 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [.], ack 37, win 291, options [nop, nop, TS val 236075895 ecr 236118882], length 0
13:52:50.614559 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [P.], seg 36:72, ack 37, win 291, options [nop,nop,TS val 236076019 ecr 236118882], length 36
13:52:50.617340 IP 10.20.4.11.ssh > 10.20.3.11.56792: Flags [P.], seg 37:73, ack 72, win 295, options [nop,nop,TS val 236119010 ecr 236076019], length 36
13:52:50.617780 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [.], ack 73, win 291, options [nop,nop,TS val 236076022 ecr 236119010], length 0
13:52:50.686251 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [P.], seq 72:108, ack 73, win 291, options [nop,nop,TS val 236076091 ecr 236119010], length 36
13:52:50.689396 IP 10.20.4.11.ssh > 10.20.3.11.56792: Flags [P.], seq 73:109, ack 108, win 295, options [nop,nop,TS val 236119082 ecr 236076091], length 36
13:52:50.689905 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [.], ack 109, win 291, options [nop,nop,TS val 236076094 ecr 236119082], length 0
13:52:50.791212 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [P.], seq 108:144, ack 109, win 291, options [nop,nop,TS val 236076196 ecr 236119082], length 36
13:52:50.794707 IP 10.20.4.11.ssh > 10.20.3.11.56792: Flags [P.], seq 109:185, ack 144, win 295, options [nop,nop,TS val 236119187 ecr 236076196], length 76
13:52:50.795250 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [.], ack 185, win 291, options [nop,nop,TS val 236076200 ecr 236119187], length 0
13:52:51.421198 IP 172.16.1.3.32846 > 172.16.1.11.bqp: Flags [F.], seg 133, ack 22, win 502, options [nop,nop,TS val 627371145 ecr 720586905], length 0
13:52:51.774181 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [P.], seq 144:180, ack 185, win 291, options [nop,nop,TS val 236077179 ecr 236119187], length 36
13:52:51.776143 IP 10.20.4.11.ssh > 10.20.3.11.56792: Flags [P.], seg 185:221, ack 180, win 295, options [nop,nop,TS val 236120169 ecr 236077179], length 36
13:52:51.776565 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [.], ack 221, win 291, options [nop,nop,TS val 236077181 ecr 236120169], length 0
13:52:51.898413 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [P.], seq 180:216, ack 221, win 291, options [nop, nop, TS val 236077303 ecr 236120169], length 36
13:52:51.901675 IP 10.20.4.11.ssh > 10.20.3.11.56792: Flags [P.], seq 221:257, ack 216, win 295, options [nop,nop,TS val 236120294 ecr 236077303], length 36
13:52:51.902097 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [.], ack 257, win 291, options [nop,nop,TS val 236077307 ecr 236120294], length 0
13:52:51.982682 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [P.], seq 216:252, ack 257, win 291, options [nop,nop,TS val 236077387 ecr 236120294], length 36
13:52:51.986850 IP 10.20.4.11.ssh > 10.20.3.11.56792: Flags [P.], seg 257:293, ack 252, win 295, options [nop,nop,TS val 236120379 ecr 236077387], length 36
13:52:51.987302 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [.], ack 293, win 291, options [nop,nop,TS val 236077392 ecr 236120379], length 0
13:52:51.990791 IP 10.20.4.11.ssh > 10.20.3.11.56792: Flags [P.], seg 293:401, ack 252, win 295, options [nop,nop,TS val 236120384 ecr 236077392], length 108
13:52:51.991178 IP 10.20.3.11.56792 > 10.20.4.11.ssh: Flags [.], ack 401, win 291, options [nop,nop,TS val 236077396 ecr 236120384], length 0

3.7.13. Для проверки HTTP возможно использовать nc на wst4:

[root@wst4]# echo Hello1 >> some.file

[root@wst4]# { printf 'HTTP/1.0 200 OK\r\nContent-Length: %d\r\n\r\n' "(wc - c < some.file)"; cat some.file; } | nc -l 8080



Для генерации HTTP запроса открыть с wst3 HTTP сессию на порт 8080 wst4. Например, с помощью curl:

[root@wst3]# curl 10.20.4.11:8080

[ivpanin@wst3 ~]\$ curl 10.20.4.11:8080 Hello1 Hello1 [ivpanin@wst3 ~]\$

Затем подключиться к vCPE-3 и проверить, что трафик переключился на корректный интерфейс (в зависимости от настроек, сделанных ранее):

tcpdump -i genev_sys_4801



На примере ниже видно, что HTTP трафик переключился с интерфейса genev_sys_4800(WAN0) на 4801 и DPI распознал HTTP трафик на нестандартном порту.

root@8000005566AAC4FD: 🔰 tcpdump -i genev_sys_4801 grep 4.11
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on genev sys 4801, link-type ENIOMB (Ethernet), capture size 262144 bytes
13:59:14.048111 IP 10.0.1.11.60286 > 10.11.12.74.zabbix-agent: Flags [S], seg 3068720290, win 64240, options [mss 1460,sackOK,TS val 4170303384 ecr 0,nop,wsc
ale 7], length 0
13:59:15.075128 IP 10.0.1.11.60318 > 10.11.12.74.zabbix-agent: Flags [.], ack 18, win 502, options [nop,nop,TS val 4170304411 ecr 3934181482], length 0
13:59:15.075660 IP 10.0.1.11.60318 > 10.11.12.74.zabbix-agent: Flags [F.], seq 66, ack 18, win 502, options [nop,nop,TS val 4170304411 ecr 3934181482], lengt
h 0
13:59:15.075764 IP 10.0.1.11.60318 > 10.11.12.74.zabbix-agent: Flags [.], ack 19, win 502, options [nop,nop,TS val 4170304411 ecr 3934181482], length 0
13:59:17.075084 IP 10.20.3.11.37720 > 10.20.4.11.8080: Flags [P.], seg 3766021115:3766021194, ack 2979344899, win 229, options [nop,nop,TS val 236462479 ecr
236505467], length 79: HTTP: GET / HTTP/1.1
13:59:17.077606 IP 10.20.3.11.37720 > 10.20.4.11.8080: Flags [.], ack 54, win 229, options [nop,nop,TS val 236462482 ecr 236505470], length 0
13:59:17.077602 IP 10.20.4.11.8080 > 10.20.3.11.37720: Flags [.], ack 79, win 227, options [nop,nop,TS val 236505471 ecr 236462479], length 0
13:59:17.077994 IP 10.20.3.11.37720 > 10.20.4.11.8080: Flags [F.], seg 79, ack 55, win 229, options [nop,nop,TS val 236462482 ecr 236505470], length 0
13:59:17.079614 IP 10.20.4.11.8080 > 10.20.3.11.37720: Flags [.], ack 80, win 227, options [nop,nop,TS val 236505473 ecr 236462482], length 0
13:59:25.852799 IP 172.16.1.3.43116 > 172.16.1.11.bgp: Flags [S], seg 3420313978, win 64240, options [mss 1460, sackOK, TS val 627765576 ecr 0, nop, wscale 7], 1

3.7.14. Возврат настроек после завершения теста.

Удалить сервис, созданный в п. 3.7.11 (при удалении отметить Remove associated service interfaces).

Убрать параметр "Unsolicited" с туннелей, добавленный в п.3.7.5.

4. Построение топологии SD-WAN сети.

В решении Kaspersky SD-WAN возможны следующие варианты топологий:

- Hub-and-Spoke. Топология по умолчанию, которая используется в том случае, если устройствам СРЕ не назначено топологических тегов. Такие устройства не устанавливают прямые туннели между собой, весь трафик в этом случае идет через шлюз SD-WAN.
- Full-Mesh. Для построения данной топологии необходимо назначить устройствам CPE одинаковый топологический тег для реализации этой топологии. Все устройства с одинаковым топологическим тегом устанавливают прямые туннели между собой.
- Partial-Mesh. Возможно, группировать устройства СРЕ путем назначения одного топологического тега одной группе устройств и другого топологического тега другой группе.
 В этом случае все устройства СРЕ из одной группы (с одинаковым топологическим тегом) пытаются установить прямые туннели между собой, а с устройствами из другой группы взаимодействуют через шлюз.



Рис. 5.1 Варианты топологий SD-WAN сети.

Для построения сетевых топологий в решении Kaspersky SD-WAN используются топологические теги, которые назначаются устройствам СРЕ.

Также устройство СРЕ может быть транзитным. В этом случае другие устройства СРЕ могут устанавливать через него туннели.

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help > Настройка топологии:

https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/250942.htm
4.1. Создание топологий Full-Mesh.

В данном сценарии настраивается топологии Full-Mesh между устройствами CPE, для этого будет добавлен одинаковый топологический тег для устройств CPE. Построенная топология будет отображена в настройках транспортного сервиса. Также будут отображены дополнительно построенные пути между устройствами CPE в разделе Сегменты.

4.1.	1. Ha	астройка топологических тегов.
Для топо Для	соз, ологі нас	дания топологии Full-Mesh устройства СРЕ должны иметь одинаковые ические теги. тройки перейти в меню СРЕ и выбрать vCPE-3.
	SD-WAN	+ CPE + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + Firmware + Certificate
∞ B D III = ⊙ ⊙ B = D		CPE Al o Watting o Configuration + Registered o Registering + Error + Unknown Alltime Lastyear Lastmonth Lastweek Lastidy [14/1/2023104] - [14/1/2023104] Al 6 + Connected 6 + Oisconnected 6 + Oisconnected 6 + Oisconnected 7 + O
Пер	ейти	и на вкладку <i>Topology</i> . Отметить <i>Override</i> и добавить тег 100 (нажать на +).
пая	ањ	Save (оркестратор применит измененные настроики к СРЕ).



	VCPE-3 Configuration Monitoring Proble Verride Configuration Transit CPE () Cogy tage () X	ens Encryption Service requests 1	Tega Scripts SD-WAN setting	a Topology Network setting	a BGPsettings OSPF Ros	xting Filters More ≠	Sure Close Actions Delete Set Location Deactivate Show password Get activation URL Unregister Open SSH console Reboot Shutdown Export network interfaces
4.1. CPI	2. Далее необ: Е. Повторить п	ходимо назнач ункт 4.1.1 для	чить тополо устройств	огический т vCPE-4, vC	тег 100 для CPE-51, vC	остальны: PE-52.	х устройств
4.1. KOH [®] Infres ← → [®] »	3. Для просмот троллер > Man tucture × + с ▲ Not secure https://10.0.1.11/ Infrestructure Resources ♀	Tpa построеннадет agement > Op infrastructure?controller/D=6527d46685 Network:resources	ной тополог pen configur 881ea44fcb695848cmode=netw 99ystem resources PAM	ии перейти ation menu.	1 в меню In (+ Domain) (+ 1	frastructure	> SD-WAN
3 B ○ ⊡ III I ⊙ ⊗ % III	All Domain Data center All resources * <u>demolab space</u> ₽ DC	Name -	Transport/service strategy Genetic VNI swapping transport	i Controller nodes	Connection type	i Chuster status i Node st DEGRADED Connec	atures : © Q Imanagement Eat Copen configuration menu Reprovision Download backup file Restore Delete Open properties
4.1. Ото топ удо	4. Выбрать для образится пост ология между бства просмот	я сервиса L2 I роенная топол СРЕ, также ус ра топологии	M2M меню погия серві тройства С можно выб	Manageme иса. На скр РЕ сохран рать Arrang	nt > View s иншоте про или туннел ge – Circle	ervice topo едставлена и до vGW(и отметить	logy. a Full-Mesh (шлюзов). Для Mame.



4.1.5. Для проверки построенных путей между устройствами СРЕ перейти на вкладку Segments. Представлен список сегментов, где видны построенные сегменты. На скриншоте ниже видно, что построены сегменты между устройствами vCPE, не проходящие через шлюзы(vGW).

Таким образом vCPE сформировали Full-Mesh между собой.

From	: То	Path count / M	ax Path number	Path type	Paths	Admin state	Oper state	Cost	Hop count	Delete	E
CPE (vCPE-4:	CPE [vGW-11:	2/8	0	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vGW-11: 8000005056AA9EA5] : 4800	up	up	10000	1		Managemen
8000005056AA35FF]	8000005056AA9EA5]		1	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vGW-11: 8000005056AA9EA5] : 4800	up	up	10000	1		
CPE [vCPE-4:	CPE [vCPE-51:	4/8	0	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-51: 8000005056AAB512] : 4800	up	up	10000	1		Managemen
8000005056AA35FF]	8000005056AAB512]		1	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vCPE-51: 8000005056AAB512] : 4801	up	up	10000	1		
			2	Auto SPF	CPE [vCPE-4: 8000005056AA35FF]: 4801 → CPE [vCPE-51: 8000005056AAB512]: 4800	up	up	10000	1		
			3	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-51: 8000005056AAB512] : 4801	up	up	10000	1		
CPE [vCPE-4:	CPE [vCPE-3:	4/8	0	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-3: 8000005056AAC4FD] : 4800	up	up	10000	1		Managemer
8000005056AA35FF]	8000005056AAC4FD]		1	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vCPE-3: 8000005056AAC4FD] : 4801	up	up	10000	1		
			2	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vCPE-3: 8000005056AAC4FD] : 4800	up	up	10000	1		
			3	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-3: 8000005056AAC4FD] : 4801	up	up	10000	1		
CPE [vCPE-4:	CPE [vCPE-52:	4/8	0	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-52: 8000005056AAC6B5] : 480	0 up	up	10000	1		Manageme
8000005056AA35FF]	8000005056AAC6B5]		1	Auto SPE	CPE 5/CPE-4:800000505684435EE1:4801 → CPE 5/CPE-52:8000005056844C6R51:480	up	UD	10000	1		in a general
			2	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vCPE-52: 8000005056AAC6B5] : 480) up	up	10000	1		
			3	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-52: 8000005056AAC6B5] : 480	1 up	up	10000	1		
CPE [vCPE-4:	CPE [vGW-12:	2/8	0	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vGW-12: 8000005056AAD2B1] : 4800	up	up	10000	1		Managemer
8000005056AA35FF]	8000005056AAD2B1]		1	Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vGW-12: 8000005056AAD2B1] : 4800	up	up	10000	1		
CPE [vGW-11:	CPE [vCPE-4:	2/8	0	Auto SPF	CPE [vGW-11: 8000005056AA9EA5]: 4800 → CPE [vCPE-4: 8000005056AA35FF]: 4800	up	up	10000	1		Manageme
8000005056AA9EA5]	8000005056AA35FF]		1	Auto SPF	CPE [vGW-11: 8000005056AA9EA5] : 4800 → CPE [vCPE-4: 8000005056AA35FF] : 4801	up	up	10000	1		
CPE [vGW-11: 8000005056AA9EA5]	CPE [vCPE-51: 8000005056AAB512]	1/8	0	Auto SPF	CPE [vGW-11: 8000005056AA9EA5] : 4800 → CPE [vCPE-51: 8000005056AA8512] : 4800	up	up	10000	1		Managemer
CPE [vGW-11:	CPE [vCPE-3:	2/8	0	Auto SPF	CPE [vGW-11: 8000005056AA9EA5] : 4800 → CPE [vCPE-3: 8000005056AAC4FD] : 4800	up	up	10000	1		Managemer
8000005056AA9EA5]	8000005056AAC4FD]		1	Auto SPF	CPE [vGW-11: 8000005056AA9EA5] : 4800 → CPE [vCPE-3: 8000005056AAC4FD] : 4801	up	up	10000	1		
CPE [vGW-11: 8000005056AA9EA5]	CPE [vCPE-52: 8000005056AAC6B5]	1/8	0	Auto SPF	CPE [vGW-11: 80000050566A99EA5] : 4800 → CPE [vCPE-52: 8000005056AAC685] : 480	0 up	up	10000	1		Manageme
CPE [vGW-11: 8000005056AA9EA5]	CPE [vGW-12: 8000005056AAD2B1]	1/8	0	Auto SPF	CPE [vGW-11: 8000005056AA9EA5] : 4800 → CPE [vGW-12: 8000005056AAD2B1] : 4800	up	up	10000	1		Managemer

4.1.6. Возврат настроек после завершения теста.

Убрать теги с СРЕ устройств, добавленные в п. 4.1.1 и 4.1.2.



4.2. Создание топологий Partial-Mesh.

В данном сценарии настраивается топологии Partial-Mesh между устройствами СРЕ. Будут сформированы 2 группы устройств СРЕ:

- vCPE-3 и vCPE-4
- vCPE-51, vCPE-52 и vCPE-4

Для построения топологии Partial-Mesh будут назначены топологические теги для устройств CPE, отдельно для каждой группы. Построенная топология будет отображена в настройках транспортного сервиса. Также будут видны дополнительно построенные пути между устройствами CPE.

4.2.1. Для создания топологии Partial-Mesh необходимо назначить устройствам СРЕ различные топологические теги в соответствии с требуемой топологией.

Необходимо перейти в меню СРЕ и выбрать vCPE-3.

	SD-WAN	+	CPE + CPE ter	nplate + UNI template -	+ SD-WAN instance template	+ SD-WAN instance pool	+ Firmware + Certificate
> () 	> 	CPE All o Waiting o Configuration - Regis All 6 - Connected 6 - Disconnected 0 DPID Model SWV	stered © Registering • Error • Connection error 0 Need upd arsion : Name : Role ;	- Unknown All time Last year ate 0 Status State Connection	Last month Last week L	ast day 14/11/2023 10:41 –	C Export to CSV 14/11/2023 10:41
© ⊡ ⊒ ⊘ &	~ 않 ~ 연 ~ 년 ~ 태	8000005056A/ x86_64 VM knaat 8000005056A/ x86_64 VM knaat	-cpe_223.07 <u>vCPE-52</u> CPE -cpe_223.07 <u>vCPE-51</u> CPE -cpe_223.07 <u>vCPE-4</u> CPE -cpe_223.07 <u>vCPE-4</u> CPE -cpe_223.07 <u>vCPE-3</u> CPE -cpe_223.07 <u>vGW-12</u> Gateway -cpe_223.07 <u>vGW-11</u> Gateway	Registered Activated Connected Registered Activated Connected Registered Activated Connected Registered Activated Connected Registered Activated Connected Registered Activated Connected	Supported Yes Supported Yes Supported Yes Supported Yes Supported Yes	Demolab Demolab Demolab Demolab Demolab Demolab Demolab Demolab Demolab Demolab Demolab Demolab	07/11/2023 17:43 07/11/2023 17:43 07/11/2023 17:43 07/11/2023 17:43 26/10/2023 16:08 26/10/2023 16:06
	0 E@						



4.2.1. Перейти на вкладку Topology. Отметить Override и добавить тег 100 (нажать на +). Нажать Save (оркестратор применит измененные настройки к CPE). Close Monitoring Problems Service requests - Tags - Scripts - SD-WAN settings Topology Network settings - BGP settings - OSPF - Routing Filters - More Encryption ✓ Override Actions Transit CPE ⑦ Delete Set location CPE Deactivate Show password Get activation URL Topology tags 🕐 100 × Unregister Open SSH cons Run scripts +Reboot Shutdown Export SD-WAN settings Export network interfaces 4.2.2. Для топологии Partial-Mesh необходимо назначить разные теги группам СРЕ. В сценарии создается 2 группы CPE: vCPE3 и vCPE-4 с тегом 100 и vCPE4, vCPE-51, vCPE-52 с тегом 200. Для их назначения повторить пункты 4.2.1-4.2.2 для остальных СРЕ со следующими значениями тегов: vCPE-51 - 200. ٠ vCPE-52 - 200. vCPE-4 – 100 и 200. 4.2.3. Просмотр сформированной топологии. Перейти в меню Infrastructure > SD-WAN контроллер > Management > Open configuration menu. Infrastr × + ← → C ▲ Not secure | https://10.0.1.11/infrastructure?controllerID=6527d46b8981ea44f + Domain + Data center 1+ VIM + Controller 1+ Sub 6 Infrastructure \gg 0 Network resources Compute resources System resources Resources Ø Transport/service strategy Controller nodes All Domain Data center Name v Connection type Cluster status Node statuses 愈口 5 SD-WAN Cluster [tenant: 6527d10f8981ea44fcb69576] Generic VNI swapping transport 10.11.11.97 (primary) Unicast Management All resources ŝ * demolab.space 0 Open configuration menu 早<u>DC</u> () ы ad backup file ≔ \bigcirc ട് D



построенные пути между устройствами СРЕ. Видно, что построенные сегменты образуют Partial-Mesh топологию в соответствии с настроенными тегами (построены сегменты между vCPE-4 и vCPE-51/52. Но не между vCPE-3 и vCPE-51/52).

legments											
From	: То	: Path count / Max	Path number	Path type	Paths	Admin state	Oper state	Cost	Hop count	Delete	
CPE [vCPE-4: 8000005056AA35FF]	CPE [vGW-11: 8000005056AA9EA5]	2/8	0	Auto SPF Auto SPF	CPE [vCPE-4: 8000005056AA35FF] :4800 → CPE [vGW-11: 8000005056AA9EA5] :4800 CPE [vCPE-4: 8000005056AA35FF] :4801 → CPE [vGW-11: 8000005056AA9EA5] :4800	up up	up up	10000 10000	1		Managem
CPE [vCPE-4: 8000005056AA35FF]	CPE [vCPE-51: 8000005056AAB512]	4/8	0 1 2 3	Auto SPF Auto SPF Auto SPF Auto SPF	CPE [vCPE-4 8000005056AA35FF] :4800 → CPE [vCPE-61 8000005056AA8512] :4800 CPE [vCPE-4 8000005056AA35FF] :4801 → CPE [vCPE-61 8000005665A48512] :4801 CPE [vCPE-4 8000005056AA35FF] :4801 → CPE [vCPE-61 800000566A48512] :4801 CPE [vCPE-4 8000005566A435FF] :4800 → CPE [vCPE-61 800000566A48512] :4801	up up up up	up up up up	10000 10000 10000 10000	1 1 1 1		Managem
CPE [vCPE-4: 8000005056AA35FF]	CPE [vCPE-3: 8000005056AAC4FD]	4/8	0 1 2 3	Auto SPF Auto SPF Auto SPF Auto SPF	CPE [vCPE-4 8000005056AA35FF]: 4800 → CPE [vCPE-3 800000566AAC4FD]: 4800 CPE [vCPE-4 8000005056AA35FF]: 4801 → CPE [vCPE-3 800000566AAC4FD]: 4801 CPE [vCPE-4 8000005056AA35FF]: 4801 → CPE [vCPE-3 800000566AAC4FD]: 4801 CPE [vCPE-4 8000005656AA35FF]: 4800 → CPE [vCPE-3 800000566AAC4FD]: 4801	up up up up	up up up	10000 10000 10000 10000	1 1 1 1		Managem
CPE [vCPE-4: 8000005056AA35FF]	CPE [vCPE-52: 8000005056AAC685]	4/8	0 1 2 3	Auto SPF Auto SPF Auto SPF Auto SPF	CPE [vCPE-4.8000005056AA35FF]:4800 → CPE [vCPE-52.8000005056AAC685]:480 CPE [vCPE-4.8000005056AA35FF]:4801 → CPE [vCPE-52.800000568AAC485]:480 CPE [vCPE-4.8000005056AA35FF]:4801 → CPE [vCPE-52.800000568AAC485]:480 CPE [vCPE-4.8000005056AA35FF]:4800 → CPE [vCPE-52.8000005056AAC485]:480	C up up) up 1 up	up up up	10000 10000 10000 10000	1 1 1 1		Managem
CPE [vCPE-4: 8000005056AA35FF]	CPE [vGW-12: 8000005056AAD2B1]	2/8	0 1	Auto SPF Auto SPF	CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vGW-12: 8000005056AAD2B1] : 4800 CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vGW-12: 8000005056AAD2B1] : 4800	up up	up up	10000 10000	1		Managem
CPE [vGW-11: 8000005056AA9EA5]	CPE [vCPE-4: 8000005056AA35FF]	2/8	0 1	Auto SPF Auto SPF	CPE [vGW-11:8000005056AA9EA5] : 4800 → CPE [vCPE-4: 8000005056AA35FF] : 4800 CPE [vGW-11:8000005056AA9EA5] : 4800 → CPE [vCPE-4: 8000005056AA35FF] : 4801	up up	up up	10000 10000	1		Managem
CPE [vGW-11: 8000005056AA9EA5]	CPE [vCPE-51: 8000005056AAB512]	1/8	0	Auto SPF	CPE [vGW-11: 80000050566AA9EA5]: 4800 → CPE [vCPE-51: 80000050566AAB512]: 4800	up	up	10000	1		Managem
CPE [vGW-11: 8000005056AA9EA5]	CPE [vCPE-3: 8000005056AAC4FD]	2/8	0 1	Auto SPF Auto SPF	CPE [vGW-11:8000005056AA9EA5] : 4800 → CPE [vCPE-3: 8000005056AAC4FD] : 4801 CPE [vGW-11:8000005056AA9EA5] : 4800 → CPE [vCPE-3: 8000005056AAC4FD] : 4800	up up	up up	10000 10000	1		Managem
CPE [vGW-11: 8000005056AA9EA5]	CPE [vCPE-52: 8000005056AAC6B5]	1/8	0	Auto SPF	CPE [vGW-11: 8000005056AA9EA5] : 4800 → CPE [vCPE-52: 8000005056AAC685] : 480	0 up	up	10000	1		Managerr
CPE [vGW-11: 8000005056AA9EA5]	CPE [vGW-12: 8000005056AAD2B1]	1/8	0	Auto SPF	CPE [vGW-11: 8000005056AA9EA5] : 4800 → CPE [vGW-12: 8000005056AAD2B1] : 4800	up	up	10000	1		Managem
CDE INCDE-51	CRE I+CRE+4	4/8	0	Auto CDE	CRE & CRE -E1 900000E0E4440E121 - 4900 -> CRE & CRE & 900000E0E4447EEE1 - 4900			10000			

4.2.5. Возврат настроек после завершения теста.

Убрать теги с СРЕ устройств, добавленные в п. 4.2.1 и 4.2.2.



4.3. Создание топологий с использованием транзитных СРЕ.

Устройства СРЕ также могут быть транзитными, в таком случае через них могут строится сегменты между другими СРЕ. В данном сценарии для демонстрации работы функционала транзитных СРЕ будет использоваться топология Partial-Mesh.

Будут сформированы 2 группы устройств СРЕ:

- vCPE-3 и vCPE-4.
- vCPE-4, vCPE-51, vCPE-52.

Каждой группе устройств СРЕ, будут назначены собственные топологические теги. Устройству vCPE-4 будет назначена транзитная роль, что позволит другим СРЕ строить туннели через данное устройство. Построенная топология будет отображена в настройках транспортного сервиса.

4.3.1. Настройка топологических тегов. Для настройки тегов и транзитной роли необходимо перейти в меню СРЕ и выбрать vCPE-4. + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + Certificate SD-WAN CPE Firmware >> C Export to CSV. CPE 0 Щ. All a Waiting a Configuration Registered a Registering Error Unknown All time Last year Last month Last week Last day 14/11/2023 10:41 - 14/11/2023 10:41 = All 6 • Connected 6 • Disconnected 0 • Connection error 0 Need update 0 ŝ ē DPID : Model : SW version : Name : Role : Status : State : Connection: Fragmentation: Usage : Transport tenant: Customer tenant: Registered 🕲 🖓 * Actions * 0 8000005056AA x86_64 VM knaas-cpe_2.23.07 vCPE-52 CPE Registered Activated Connected Supported Yes Demolab Demolab 07/11/2023 17:43 ရှိဖို့ (8000005056A/ x86_64 VM knaas-cpe_2.23.07 vCPE-51 CPE Registered Activated Connected 07/11/2023 17:43 Demola Demolab ы R 8000005056AA x86_64 VM knaas-cpe_2.23.07 vCPE-4 CPE Registered Activated Connected Supported Yes 07/11/2023 17:43 Demolab Demolab := 8000005056A/ x86_64 VM knaas-cpe_2.23.07 vCPE-3 CPE Registered Activated Connected 07/11/2023 17:42 Yes Demolab Demolab 0 9 8000005056A- x86_64VM knaas-cpe_2.23.07 vGW-12 Gateway Registered Activated Connected Supported Yes Demolab Demolab 26/10/2023 16:08 റ്റ 8000005056A/ x86_64 VM knaas-cpe_2.23.07 vGW-11 Gateway Registered Activated Connected Supported Yes Demolab 26/10/2023 16:06 Demolab 2 n **\$** (Teo 4.3.2. Перейти в раздел Topology. Отметить Override, Transit СРЕ и добавить теги 100 и

4.3.2. Перейти в раздел Topology. Отметить Override, Transit CPE и добавить теги 100 и 200 (нажать на +). vCPE-4 выполняет транзитную роль и, благодаря этой настройке туннели между другими CPE будут также проходить через vCPE-4, а не только через шлюзы (vGW-11 и vGW-12). Нажать Update configuration (оркестратор применит новые настройки к CPE).



	Save Close
VCPE4 Configuration Monitoring Problems Encryption Service requests Tags Scripts SD-WAN settings Topology Networksettings BGP-settings OSPE Routing Filters More* Weight Transl CPE® Translope Topology Tags © Topology Tags Tags Topology Tags Topolo	Actions Delete Set location Deactivate Show password Get activation URL Urregister Open SSH console Run scripts Reboot Shutdown Export SD-WAN settings Export network interfaces
 4.3.3. Для топологии необходимо назначить разные теги разным группам сценарии создается 2 группы СРЕ: vCPE3 и vCPE-4 с тегом 100 и vCPE4 vCPE-52 с тегом 200. Для назначения тегов пункты 4.3.1 - 4.3.2 для остал следующими значениями тегов (эти СРЕ не будут транзитными для них нотмечать Transit CPE): vCPE-3 – 100. 	і СРЕ. В , vCPE-51, тьных СРЕ со не требуется

- vCPE-51 200.
- vCPE-52 200.

4.3.4. Проверка построенной топологии.

Перейти в меню Infrastructure > SD-WAN контроллер > Management > Open configuration menu.

From	i To i	Number of paths	# Path type	Transport paths	Administrative state	Operational state	Cost	Hop count	Delete	
8000005056AAB5	12 8000005056AAC68	81	Auto SPF	CPE [vCPE-51: 8000005056AAB512] : 4801 → CPE [vCPE-52: 80000050	56 up	up	10000	1		
			2 Auto SPF	CPE [vCPE-51: 8000005056AAB512] : 4801 → CPE [vCPE-52: 80000050	56 up	up	10000	1		
			3 Auto SPF	CPE [vCPE-51: 8000005056AAB512] : 4800 → CPE [vCPE-52: 80000050	05r up	up	10000	1		
OPE [VOPE-51	CPE [vGW-12:	2/8	0 Auto SPF	CPE [vCPE-51: 8000005056AAB512] : 4800 → CPE [vGW-12: 80000050	567 up	up	10000	1		Manageme
8000005056AAB5	12 8000005056AAD28	31	Auto SPF	CPE [vCPE-51: 8000005056AAB512] : 4801 → CPE [vGW-12: 800000505	6A up	up	10000	1		
OPE [VOPE-3:	CPE [VCPE-4:	4/8	0 Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4800 → CPE [vCPE-4: 800000505	56/ up	up	10000	1		Manageme
8000005056AAC4	FE 8000005056AA35F	F	Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4801 → CPE [vCPE-4: 800000505	6A up	up	10000	1		
			2 Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4801 → CPE [vCPE-4: 800000505	6A up	up	10000	1		
			3 Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4800 → CPE [vCPE-4: 800000505	567 up	up	10000	1		
CPE [VCPE-3:	CPE [vGW-11	2/8	0 Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4800 → CPE [vGW-11: 800000505	6A up	up	10000	1		Manageme
8000005056AAC4	FI 8000005056AA9EA	et i i i i i i i i i i i i i i i i i i i	Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4801 → CPE [vGW-11: 800000505	5A, up	up	10000	1		
CPE [vCPE-3: CPE [vCPE-51: 4 80000050566AAC4FI 8000005056AAB512	4/8	0 Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4800 → CPE [vCPE-4: 80000050 CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-51: 80000050	i6/ up 56.	up	20000	2		Manageme	
			Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4800 → CPE [vCPE-4: 80000050 CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vCPE-51: 800000505	567 up 164	up	20000	2		
			2 Auto SPF	CPE [vCPE-3: 80000050566AAC4FD] : 4801 → CPE [vCPE-4: 800000505 CPE [vCPE-4: 80000050566AA35FF] : 4801 → CPE [vCPE-51: 800000505	6A up 6A	up	20000	2		
			3 Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4801 → CPE [vCPE-4: 800000505 CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-51: 80000050	6A up 56.	up	20000	2		
CPE [vCPE-3: 8000005056AAC4	CPE [vCPE-52: FE 8000005056AAC6E	4/8	0 Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4800 → CPE [vCPE-4: 80000050 CPE [vCPE-4: 8000005056AA35FF] : 4800 → CPE [vCPE-52: 80000050	567 up 56	up	20000	2		Manageme
			Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4801 → CPE [vCPE-4: 800000505 CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vCPE-52: 80000050	6A up 56/	up	20000	2		
			2 Auto SPF	CPE [vCPE-3: 80000050566AAC4FD] : 4800 → CPE [vCPE-4: 80000050 CPE [vCPE-4: 8000005056AA35FF] : 4801 → CPE [vCPE-52: 80000050	i6/ up ნბ	up	20000	2		
			3 Auto SPF	CPE [vCPE-3: 8000005056AAC4FD] : 4801 → CPE [vCPE-4: 800000505	6A up	up	20000	2		

4.3.5. Возврат настроек после завершения теста.

Убрать теги с СРЕ устройств, добавленные в п. 4.3.1-4.3.3.

5. Работа с СРЕ устройствами.

5.1. Централизованное обновление firmware СРЕ устройств.

Kaspersky SD-WAN поддерживает централизованное обновление firmware («прошивок») на устройствах СРЕ. Перед установкой новой версии прошивки ее необходимо загрузить через вебинтерфейс оркестратора. Прошивки распространяются в виде архивов в формате TAR.GZ. Каждый архив содержит саму прошивку, а также файл с метаданными в формате yml. Параметры, указанные в файле с метаданными, импортируются в веб-интерфейс оркестратора при добавлении архива с прошивкой.

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help > Прошивки: <u>https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/247435.htm</u>

В данном сценарии рассматривается централизованное обновление firmware CPE.

5.1.1. Загрузка новой версии firmware.

Для загрузки новой версии firmware необходимо перейти в меню SD-WAN.

	SD-WAN		+ CPE -	+ CPE templa	ate + UNIte	amplate +	- SD-WAN instance to	emplate + SD-WAN	instance pool -	- Firmware -	- Certificate
\$ \$ 0 !!! = O \$ 5 = D \$	◈ ᆌ《 疁《 꽃○ ᠿᆞ ᠿᆞ 맴아 짧॰ ☞.	CPE All o Waiting o Configuration All 6 · Connected 6 · Disco DPID Model B000005056A2 ×86,6 B000005056A2 ×86,6 B000005056A2 ×86,6 B000005056A2 ×86,6 B000005056A2 ×86,6 B000005056A2 ×86,6	on • Registered o Registering nnected 0 • Connection error 0 1 SW version Name 4 VM knass-cpe_2.23.07 vCPE-52 4 VM knass-cpe_2.23.07 vCPE-4 4 VM knass-cpe_2.23.07 vCPE-3 4 VM knass-cpe_2.23.07 vCPE-3 4 VM knass-cpe_2.23.07 vCPE-3 4 VM knass-cpe_2.23.07 vGW-12	+ Error - Ur Need update (Role) Stat CPE Reg CPE Reg Gateway Reg Gateway Reg	nknown All tin o tus State i gistered Activated gistered Activated gistered Activated gistered Activated	e Lastyear Connection Connected Connected Connected Connected Connected	Lastmonth Lastv Fragmentation Usa Supported Yes Supported Yes Supported Yes Supported Yes	veek Last day 14/11/ age Transport tenant Demolab Demolab Demolab Demolab Demolab	2023 10:41 – 1 Customer tenant ; Demolab Demolab Demolab Demolab Demolab	C 4/11/2023 10:41 Registered ① Q.* 07/11/2023 17:43 07/11/2023 17:43 07/11/2023 17:43 07/11/2023 17:42 26/10/2023 16:08 26/10/2023 16:06	Export to CSV

Нажать на кнопку +*Firmware* и в диалоговом окне загрузить файл с новой версией ПО для СРЕ.

Дождаться окончания загрузки (статус будет отображаться вместо кнопки +*Firmware*).

SD-WAN	+ CPE + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + Firmware + Certificate
>>	CPE Expertito CSV.
6	All • Waiting • Configuration • Registering • Error • Unknown All time Last work Last day 07/11/2023 18:06 All • Consected 6 • Disconcented 0 • Openeted 0 • Openeted 0 • Openeted 0 • Openeted 0
¢]	DPID : Model ; SW version Name ; Role ; Status ; State ; Connection ; Fragmentation ; Usage ; Transport tenant ; Customer tenant ; Registered 🔞 Q 🔹 Actions * ;
୶୲ଌ	B0000050566AAC68 x86_64 VM knass-cpe_2.23.07 release 23 bios amd64 vCPE-52 CPE Registered Activated Connected Supported Yes Demolab 07/11/2023 17.43
£	• B000005056AAB5fit x86,64 VM knaas-cpe,2.23.07 release 23 bios at € → × • B000005056AAB5fit x86,64 VM knaas-cpe,2.23.07 release 23 bios at € → × × • B000005056AAB5fit x86,64 VM knaas-cpe,2.23.07 release 23 bios at ← → ↑ > Sourch CPE firmware ✓ ▷ Sourch CPE firmware ∅
i G	B0000050564AC4F x86_64VM knaas-cpe_2.23.07 release 23 bios a Organize New folder Deter modified Type Size
	B0000056656A0228 x86,64 VM knase-cpc.223.07release 23 bios an GM 21 bios and CM 21 bios and
۰ ١	Zabita template Shink K Jo Opices
	Destrop
	→ Muse ■ Returns ■ Voteos → Local Dat(K) →
	CO Drive (D) File name (page-cose 22107 referee 23100 xmm044 leaguery en-1/5 nr-8011ar zz:) File name (page-cose 22107 referee 23100 xmm044 leaguery en-1/5 nr-8011ar zz:)
	One Carel

5.1.2. Просмотр СРЕ, доступных для обновления.

Перейти в меню СРЕ. Откроется список СРЕ.

СРЕ, для которых доступна новая версия ПО, будут выделены цветом в колонке SW version. Новая версия firmware доступна для всех СРЕ.

SD-WAN	+	+ CPE Device + CPE Tem	plate + UNI template +	SD-WAN Instance template	+ SD-WAN Instances Pool	Firmware + Certificate
>>	CPE Inventory					C Export to CSV
	All c Waiting c Configuration • Reg All c • Connected c • Disconnected 0	sistered o Registering • Error • Connection error 0 Need upde	Unknown All time Last year ate 6	Last month Last week L	ast day 27/06/2023 13:28 – 2	7/06/2023 13:28
¢	DPID : Model : SWV	Version : Name : Role : :	Status : State : Connection :	Fragmentation : Usage :	Transport Tenant : Customer Tenant :	Registered - 🛞 Q* Actions*
ရွှိန	• 8000005056A/ x86_64VM knaa	as-cpe_2.23.03 CPE-52 CPE	Registered Activated Connected	Supported Yes	Demolab Demolab	18/05/2023 15:28
0	• 8000005056A/ x86_64VM knas	as-cpe_2.23.03 CPE-51 CPE	Registered Activated Connected	Supported Yes	Demolab Demolab	18/05/2023 15:27
<u> </u>	• 8000005056A/ x86_64VM knas	as-cpe_2.23.03 CPE-4 CPE	Registered Activated Connected	Supported Yes	Demolab Demolab	18/05/2023 15:27
1	• 8000005056AA x86_64VM knaa	as-cpe_2.23.03 CPE-3 CPE	Registered Activated Connected	Supported Yes	Demolab Demolab	18/05/2023 15:27
Ģ	• 8000005056A/ x86_64 VM knaa	as-cpe_2.23.03 GW-12 Gateway	Registered Activated Connected	Supported Yes	Demolab Demolab	18/05/2023 14:52
	• <u>8000005056A/</u> x86_64VM knaa	as-cpe_2.23.03 IGW-11 Gateway	Registered Activated Connected	Supported Yes	Demolab Demolab	18/05/2023 14:52
∰ 1						
1						

5.1.3. Создание задания (task) на обновление firmware.

В CPE Inventory отметить слева все CPE, для которых требуется обновить прошивку.

SD-WAN	+ CPE + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + Fit	rmware + Certificate
>>	CPE	Export to CSV
<u>ш</u>	All o Waiting o Configuration - Registered o Registering - Error - Unknown All time Last year Last month Last week Last day 07/11/2023 18:06 - 07/11/2023 18:06	
¢.	PDD - Model - SWversion - Name - Role - Status - State - Connection - Fraementation - Usage - Transport tenant - Gustomertenant - Review	ered for O v Actions v :
୍ଦ୍ଧ	S000005056AAC6E x86,64 VM knass-cpc.22307relesse 23.bios.amd64 vCPE-52 CPE Registered Activated Connected Supported Yes Demolab Demolab 07/11/2	2023 17:43
	- 📝 2000005056AAB512 x86_64 VM knass-cpe_2.23.07release.23.bios.amd64 VOPE-51 CPE Registered Activated Connected Supported Yes Demolab Demolab 07/1/2	2023 17:43
힌	Comparison of the state of	2023 17:43
Ģ	Comparison of the state of	2023 16:08
~	Nov 20000050566AA9EA x86_64VM knass-cpe_223.07relesse 23.bios.amd64 VGW-11 Gateway Registered Activated Connected Supported Ves Demolab Demolab 26/10/	2023 16:06
۰ ش		
2 2		
Con	NARA R MOLUO RUGRATI, Actions > Firmware undate	
Clip	aba B Meho Booparb Actions > Finnware upuale.	
SD-WAN	+ OPE + OPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + F	Firmware + Certificate
SD-WAN	+ OPE + OPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + F	Firmware + Certificate
SD-WAN	+ OPE + OPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + P	Firmware + Certificate
SD-WAN	+ OPE + OPE template + SD-WAN instance template + SD-WAN instance template + SD-WAN instance pool + P CPE All © Waiting © Configuration • Registered © Registering • Error • Unknown All time Last year Last month Last week Last day 07/11/2023 18.06 - 07/11/2023 18.06 All 6 • Connected 6 • Disconnected 0 • Connection error 0 Need update 0	Firmware + Certificate
SD-WAN	PPD (Model ; SWversion Name Role Status State Connection Fragmentation Usage Transport tenant Customertenant Regis	Firmware + Certificate
SD-WAN	+ OPE + CPE template + SD-WAN instance template + SD-WAN instance pool + F CPE All or Waiting a Configuration - Registering - <t< td=""><td>Firmware + Certificate</td></t<>	Firmware + Certificate
SD-WAN	+ OPE + OPE template + UNitemplate + SD-WAN instance pool + F CPE All o Waiting © Configuration • Registered © Registering • Error + UNitemplate + SD-WAN instance pool + F All o Waiting © Connected © • Registered © Registering • Error + UNitemplate Last week Last day O7/11/2023 18:06 - 07/11/2023 18:06 07/11 07/11	Firmware + Certificate
SD-WAN	+ OPE + CPE template + UNI template + 5D-WAN instance template + 5D-WAN instance pool + F CPE All o Waiting © Configuration • Registered © Registering • Error • Unknown All time Last year Last month Last week Last day O7/11/2023 18.06 - 07/11/2023 18.06 07/11/2023 18.06 07/11/2023 18.06	Firmware + Certificate
SD-WAN	+ OPE + OPE template + UNI template + 50-WAN instance template + 50-WAN instance pool + F CPE All = Waiting = Configuration + Registered = Registering + Error + Unknown All time Last year Last month Last week Last day 07/11/2023 18:06 - 07/11/2023 18:06 All = + COnnected + Disconnected - Connected - Connected + Disconnected - Connected + Disconnected + Disconnect + Disconnected + Disconnected + Disconnected + Discon	Firmware + Certificate
5D-WAN	+ OPE + OPE template + UNI template + 50-WAN instance template + 50-WAN instance pool + F CPE All or Waiting © Configuration + Registered © Registering + Error + Unknown All time Last year Last month Last week Last day 07/11/2023 18:06 - 0000000556AAGE = 866,64 VM kinase-ope,223:07 release 23:00 amdd4 VOPE-3 OPE Registered Activated Connected Supported Yes Demolab 07/11 V 80000000556AAGE = 866,64 VM kinase-ope,223:07 release 23:00 amdd4 VOPE-3 OPE Registered Activated Connected Supported Yes Demolab 07/11 V 80000000556AAGE = 866,64 VM kinase-ope,223:07 release 23:00 amdd4 VOPE-3 OPE Registered Activated Connected Supported Yes Demolab 07/11 V 80000000556AAGE = 86	Firmware + Certificate
	CPE + OPE + OPE template + UNitemplate + SD-WAN instance template + SD-WAN instance pool + F CPE All or Waiting a Configuration + Registering + Eror + Unknown All time Lastyear Last month, Lastweek Last day (07/11/2023 18:06 - 07/11/2023 18:06 All or - Onected + Disconnected • Disconnected • Disconnection error 0 Need update 0 Yes Demolab Demolab (7/1 Yes Demolab Demolab 07/1 Model ; SWversion ; Name ; Role ; Status ; State ; Connection ; Fragmentation ; Usage ; Transporttemant ; Customertemant ; Roges Yes Demolab Demolab 07/1 Yes Demolab Demolab 0	Firmware + Certificate
$\label{eq:sd-ward} \text{SD-WAR} \qquad \qquad$	+ OPE + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + F CPE All o'Waiting o'Configuration Registering + Enror - Ornected 07/11/2023 18:06 - O'TI/2023 18:06 O'TI/2023 18:06 O'TI/2023 18:06 O'TI/2023 18:06 O'TI/2023 18:06 O'TI/2023 18:06	Firmware + Certificate
SD-WAN 🔌 🗐 · 🦉 · 🖧 · 🤤 · 🎝 - ปြ · ปြ · 🛱 ·	+ OPE + OPE template + UNI template + 50-WAN instance template + 50-WAN instance pool + F CPE All o Waiting © Onfiguration - Registered 0 Registered 0 Registered 0 Commetted - 07/1/202318.06 07/1/202318.06 07/1/202318.06 07/1 07/1 07/1 07/1 07/1 07/1 <t< td=""><td>Firmware + Certificate</td></t<>	Firmware + Certificate
SD-WAN	+ OPE + OPE template + UNI template + 50-WANI instance template + 50-WANI instance pool + F CPE All or Visiting © Connection - Or/II/2023 18:06 Or/III/2023 18:06 Or/II/2023 18:06 Or/III	Firmware + Certificate
$\begin{array}{c c} & & & \\ &$	+ OPE + OPE template + SD-WAN instance template + SD-WAN instance pool + F CPE All bine Last year Last year Last month Last week Last day O7/1/2023 18:06 - O7/1/2023 18:06 O/1/1 O O000000000000000000000000000000000000	Firmware + Certificate
	+ OPE + CPE template + SD-WAN instance template + SD-WAN instance pool + F CPE All or Wasting of Configuration + Registered of Registering + Enror + Unknown All time Last year Last week Last day 07/11/202318:06 - 07/11/202318:06 All or Ommented 6 + Otscommented 0 + Connection error 0 Need update 0 . Mile + Status : Status : Status : CPE • B0000005056AAADCE: x86,44VM Inasas-cps.22307release 23 bios amd64 vOPE-50 CPE Registered Activated Connected Supported Yes Demolab Demolab 0/7/1 • B0000005056AAADE: x86,44VM Inasas-cps.22307release 23 bios amd64 vOPE-50 CPE Registered Activated Connected Supported Yes Demolab 0/7/1 • B0000005056AAADE: x86,44VM Inasas-cps.22307release 23 bios amd64 vOPE-50 CPE Registered Activated Connected Supported Yes Demolab D/7/1 • B0000005056AAADE: x86,44VM Inasas-cps.2307release 23 bio	Firmware + Certificate
SD-WAN \gg 4 3 3 3 3 3 3 3 3 3 3	+ CPE + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + F	Firmware + Certificate
	+ OPE + OPE (mighter) + SD-WAN instance templete + SD-WAN instance pool + F	Firmware + Certificate
SD-WAN	+ OFE + OFE template + UNItemplate + 50-WAN instance template + 50-WAN instance + 5	Firmware + Certificate

CPE CPE CPE Consected a Consected a Registered & Regi
Completion date and time Save configuration Transforme update Configuration Completion date and time Configuration

Отметить CPE для обновления и нажать Schedule.

SD-WAN		+ CPE + CPE template + UNI template + SD-WAN instance template + SD-WAN instance pool + Firmware + Certificate
>>>	CPE	C Export to CSV.
6	All c Waiting c Configuration +	Firmware update ×
¢	DPID : Model	Update on following CPEs: 4/6 items Customer tenant : Registered @ Q * (Actions*) :
ଶ୍ୱାନ୍ତ	• 🗹 8000005056AAC68 x86_64	Or PD I Minima I Minima <t< th=""></t<>
0	• 🗹 8000005056AAB512 x86_64	cpe_2.23.07 release 23.bi Demolab 07/11/2023.17.43
	• 🗹 8000005056AA35FF x86_64	Image: Source of the second
6	• 🗹 8000005056AAC4FL x86_64	✓ 80000050564A35FF x86_64VM vCPE-4 knass- Demolab 07/11/202317.42
1	• 8000005056AAD2B x86_64	cpe_2.23.07/release 23.01 Demotab 26/10/2023.16.08
÷.	• <u>8000005056AA9EA</u> : x86_64	Do not update on following CPEs: 0 item 0 item
0		: DPID ; Model ; Name ; SW version ; Tenant ; Reason ;
2		
(FQ		
1		
		Cancel Back Schedule

5.1.4. Проверка статуса задачи

Перейти в меню Scheduler.

Найти в списке созданную задачу и посмотреть статус. После успешного выполнения задачи, её статус изменится на Done.

	Scheduler							+ Delayed task
>>	Tasks .>>	All						C
Ø	All >	All Pending Running Queued	Error Done All time Last year	Last month Last week Last day	06/11/2023 21:06 - 07/11/202	13 18:06		
تا مہ	Delayed sc		Name	User	Created	Status	Scheduled ~	Actions *
0	Delayed fi	655362563d06c16e5f32961d	Firmware upgrade	admin	14/11/2023 15:04	Running	07/11/2023 18:06	
()								
ы								
≣								
0								
<u>6</u> 5								
e,								
		Running					~	Save Close
		Name	Version					Actions
		Firmware upgrade	knaas-ope_2.23.07.release 23.bios.a V					
		Completion date and Save conf	iguration ⑦ Force update ⑦					
		07/11/2023 18:06						1

5.1.5. Просмотр версий firmware CPE после обновления

Перейти в меню СРЕ.

CPE Inventory					Export to CSV
All o Waiting o Configuration • Registered o Registering • E All 6 • Connected 4 • Disconnected 2 • Connection error 0 Nee	ror • Unknown I update 2	All time Last year Last m	onth Lastweek Lastday	27/06/2023 13:47 -	27/06/2023 13:47
DPID : Model : SWVersion :	Name : Role :	Status : State : Conn	ectic: Fragment: Usage	Transport Te Customer Te	Registered - 🕲 Q 🕷 Actions 🔻
8000005 x86_64 VM knaas-cpe_2.23.03.release.33.bios.amd64	VCPE-52 CPE	Registered Activated Conn	ected Supported Yes	Demolab Demolab	18/05/2023 15:28
8000005 x86_64 VM knaas-cpe_2.23.03.release.33.bios.amd64	VCPE-51 CPE	Registered Activated Conn	ected Supported Yes	Demolab Demolab	18/05/2023 15:27
8000005 x86_64 VM knaas-cpe_2.23.03.release.33.bios.amd64	VCPE-4 CPE	Registered Activated Conn	ected Supported Yes	Demolab Demolab	18/05/2023 15:27
2000005 x86_64 VM knaas-cpe_2.23.03.release.33.bios.amd64	VCPE-3 CPE	Registered Activated Conn	ected Supported Yes	Demolab Demolab	18/05/2023 15:27

Отобразится список CPE, в колонке SW Version будет указана новая версия прошивки, также, значение версии не будет выделено цветом.

Обновление успешно завершено.

5.2. Резервирование устройств СРЕ с использованием VRRP.

Kaspersky SD-WAN поддерживает установку нескольких устройств CPE на площадках для обеспечения высокой доступности. Одним из вариантов организации высокой доступности является использование протокола VRRP (Virtual Router Redundancy Protocol).





Взаимодействие по протоколу VRRP может быть настроено между несколькими устройствами CPE, а также между устройством CPE и сторонним маршрутизатором.

Для настройки VRRP необходимо создать экземпляры VRRP (VRRP instances), которые определяют, какие устройства CPE объединяются в виртуальные маршрутизаторы для обеспечения высокой доступности. При создании каждого экземпляра VRRP указываются общие параметры протокола VRRP, такие как идентификатор VRID (Virtual Router Identifier) виртуального маршрутизатора и виртуальный IP-адрес для сетевого интерфейса устройства CPE.

Экземпляры VRRP могут быть объединены в группы для синхронизации их работы. Таким образом, если в одном из экземпляров VRRP, входящих в группу, произойдет изменение основного VRRP-маршрутизатора, то основной маршрутизатор изменится во всех остальных экземплярах VRRP в группе.

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help > Протокол VRRP: <u>https://support.kaspersky.com/help/SD-WAN/2.1/ru-RU/246585.htm</u>

В данном сценарии будет настроен экземпляр VRRP между vCPE-51 и vCPE-52 и проверена работа протокола путем отключения lan интерфейса(eth2) между vCPE-51 и wst5.



5.2.1. Настройка адреса lan интерфейса.

Для выполнения сценария необходимо изменить IP-адрес lan интерфейса на устройстве vCPE-51. Перейти в меню SD-WAN, открыть CPE templates и выбрать vCPE-51

SD-WAN		+ CPE Device	+ CPE Template + UNI	emplate + SD-WAN Instance ter	mplate + SD-WAN Instances Pool	+ Firmware	+ Certificate
>>	CPE templates						
<u></u>	All Used All time Last year Last month	stweek - Last day - 18/07/2023 10:28	- 18/07/2023 10:28				
, A	ID : Name		: Usage	Updated ~	: User	: Owner	© Q₹
<u>م</u>	64abb7a2617992266c8a7580 vCPE-51		Yes	18/07/2023 10:31	admin	-	
25	64abb7c3617992266c8a7583 vCPE-52		Yes	10/07/2023 10:48	admin	-	
0	64abb783617992266o8a757d vCPE-4		Yes	10/07/2023 10:47	admin	-	
£	64abb771617992266c8a757a vCPE-3		Yes	10/07/2023 10:47	admin	-	
1	64abb754617992266c8a7577 vGW-12		Yes	10/07/2023 10:46	admin	-	
G 1	64abb6c8617992266c8a7573 vGW-11		Yes	10/07/2023 10:44	admin	-	
P 0°							
0 0							
1						Save	Close
	Information - Multipathing - Deactivation	Encryption Configurations SD-WA	N Settings Topology Network S	ttings BGP Settings BFD Settings	Static Routes VRRP More *		
	+ Add an interface					Actions	
	Alias : Interface Nat	ne	Protocol	Enable automatically	·	: Delete	
	lan eth2		Static address IPv4	Yes	Edit Remove	Export Clone	

Открыть вкладку Network settings. Для интерфейса lan выбрать Edit.

35	: Interface Name	Protocol	Enable automatically		Delete
	eth2	Static address IPv4	Yes	Edit	Export
				Disable	Export SD-WAN Configurat Export Network Settings
erlay	overlay	Static address IPv4	Yes	Edit Remove Disable	Show Attached CPE
wanO	eth0	DHCP client	Yes	Edit Remove Disable	
van1	eth1	DHCP client	Yes	Edit Remove Disable	

SD-WAN			+ CPE Device + CPE Ten	mplate + UNI template	+ SD-WAN Instance template	+ SD-WAN Instances Pool	+ Firmware + Certificate
»	VCPE-51	<u>Deactivation</u> Encryption	Edit		tings Static R	outes VRRP More *	Save Close
	+ Add an interface Alias	; Interface Name	Alias	Interface Name ⑦ eth2	itically		Actions Delete Import
e Se Se	lan	eth2	Type Bridge ⑦ Protocol			Edit Remove Disable	Export Clone Export SD-WAN Configuration
°	overlay	overlay	Enable automatically ⑦ Force link ⑦			Edit Remove	Export Network Settings Show Attached CPE
G ₁	sdwan0	eth0	IPv4 address ⑦ 10.20.5.3	IPv4 netmask ⑦ 255.255.255.0	_	Edit Remove	
000	sdwan1	eth1	IPv4 gateway ⑦	IPv4 broadcast ⑦		Disable Edit Remove	
0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			+ Add Override MAC address ⑦ Override	e MTU ② Use gateway	y metric ⑦	Disable	
1			DHCP Server				
			Disabled		~		
				Close	Save		
Second Second							
Наж	ать Save в ша	блоне CF	ΡĒ.				
Наж	ать Save в ша	блоне CF	PE.	pology Network Settings BGP S	Settings BFD Settings Static Ro	utes VRP More *	Save Close
Hax	кать Save в ша vcPE-5 ^{l linuxe} information Multipathing + Add an interface Alas	облоне СF	Configurations SD-WAN Settings To	pology (Network Settings) BGPS	BETD Settings Static Ro	utes <u>VR6P</u> More *	Save Close Actions Delists
Hax	кать Save в ша vcpe.st information + Add an interface Alas	облоне СF	PE. Configurations SD-WAN Settings To ; Prot Stat	pology (Network Settings) BGP S locol ic address IPv4	Settings BFD Settings Static Ro : Enable automatically Yes	utes VRRP More * I Edit Remove Deable	Actions Delete Import Export Clone Export SD-WAN Configuration
Ha x > 4	CATE Save B max vcPE-51 Information Multiparting + Add an interface Alas Jan overlay	облоне СР Desettvation Encryption interface Name eth2 overlay	Configurations SD-WAN Settings To ; Prot Stat	pology (Network Settings) BGPS cocol ico address IPv4	Settings BFD Settings Static Ro : Enable automatically Yes Yes	utes VR8P More * I I Edit Remove Deable Deable Deable	Save Close Actions Delete Import Export Clone Export S-WAN Configuration Export Network Settings Show Attached CPE
Ha x > ¹	CATE Save B Luca Nultipating + Add an interface Alas lan overlay sdwan0	В БЛОНЕ СГ Deactivation Encryption i Interface Name eth2 overlay eth0	DE. <u>Configurations</u> SD-WAN Settings To : Prot Stat Stat	pology (Network Settings) BGP S locool lo address IPv4 sko address IPv4 SP client	Settings BFD Settings Static Rd : Enable automatically Yes Yes	utes VRRP More + I Edit Remove Disable Edit Remove Disable	Save Close Actions Delete Import Export Clone Export SD-WAN Configuration Export Network Settings Show Attached CPE
Ha x > 4 · • • * · 4 · • *	CATE Save B max recent and an interface Add an interface Add an interface Adds lan overlay sdwem0 idwan1	В БЛОНЕ СГ Deactivation Encryption i Interface Name eth2 overlay eth0 eth1	Configurations SD-WAN Settings To , Prot Stat Stat DHC	pology Network Settings BGP S tocol io address IPv4 to address IPv4 SP client SP client	bettings BED Settings Static Ro E Enable automatically Yes Yes Yes Yes	utes VIRP More * i Edit Remove Disable Edit Edit Remove Disable	Save Close Actions Delete Import Export Close Export SD-WAN Configuration Export Network Sattings Show Attached OPE
Hax > 1, , , , , , , , , , , , , , , , , , ,	CATE Save B max	В В Deactivation Encryption i Interface Name eth2 overlay eth0 eth1	Configurations SD-WAN Settings To i Prot Stat Stat DHC	pology Network Settings BGP S tocol ice address IPv4 ice address IPv4	bettings BED Settings Static Ro E Enable automatically Yes Yes Yes Yes	utes VRRP More *	Save Close Actions Delete Import Export Close Export SD-WAN Configuration Export Network Sattings Show Attached OPE
Hax > 4 · · · · · · · · · · · · · · · ·	CATE Save B use Information Multipathing + Add an interface Allas overlay sdwan0 	блоне СК Deactivation Encryption eth2 overley eth0 eth1	Configurations SD-WAN Settings To ; Prot Stat 	pology Network Settings BGP s tocol ic address IPv4 at address IPv4 3P client 3P client	Settings BFD Settings Static Ro Enable automatically Yes Yes Yes Yes	utes VRRP More * : : : : : : : : : : : : : : : : : : :	Sure Close Actions Delete Inport Export Clone Export SD-WAN Configuration Export Network Settings Show Attached CPE
На≫ ≫ ≟。 嗯。 ╬。 ♀- ♀- 哚。 隠・ ■-	CATE SAVE B LUCA Information Multipathing + Add an interface Allas overlay sdwan0 	аблоне СК Deactivation Encryption eth2 overlay eth0 eth1	Configurations SD-WAN Settings To Configurations SD-WAN Settings To Front State State DHC	pology Network Settings BGP s tocol ic address IPv4 at address IPv4 3P client 3P client	Settings BFD Settings Static Ro Enable automatically Yes Yes Yes Yes	utes VRRP More * : : : : : Edit Remove Disable Edit Remove Disable Edit Remove Disable	Sure Close Actions Delete Inport Export Clone Export SD-WAN Configuration Export Network Settings Show Attached OPE



5.2.2. Настройка экземпляра VRRP.

Перейти в меню SD-WAN, открыть CPE templates и выбрать vCPE-51

	All Used All time Last year					
		Last month Last week Last day 18/	/07/2023 10:28 - 18/07/2023 10:28			
	10	Name	- Jieare	. Undated	llear	. Ounor da
20	1D 64abb7a2617992266c8a7580	vCPE-51	Yes	18/07/2023 10:31	admin	- Owner 881
ŝ	64abb7c3617992266c8a7583	vCPE-52	Yes	10/07/2023 10:48	admin	-
	64abb783617992266c8a757d	VCPE-4	Yes	10/07/2023 10:47	admin	
<u>_</u>	64abb771617992266c8a757a	VOPE-3	Yes	10/07/2023 10:47	admin	
÷	64abb754617992266c8a7577	vGW-12	Yes	10/07/2023 10:46	admin	
5	64abb6c8617992266c8a7573	<u>vGW-11</u>	Yes	10/07/2023 10:44	admin	-
5						
1						
\$						
>	Is in use					Save
\$	VCPE-51	ng . Deactivation . Encryption . Configurat	tions SD-WAN Settings Topology Network Sett	ings BGP Settings BFD Settings	Static Routes VRRP Mo	ire *
-	+ Add an interface					Actions
	Alias	: Interface Name	: Protocol	Enable automaticall	/ :	: Import
	lan	eth2	Static address IPv4	Yes	Edit	Export
					Remove Disable	Export SD-W
	vCPE-51	ctivation Encryption Configurations	SD-WAN SettingsTopologyNetwork Settings	BGP Settings . BFD Settings . 5	Static Routes VRRP* More	* Actions
RRP Insta	ances VRRP Groups					Actions Delete
nabled	~					Import Export
u need to cr	reate at least one instance					Clone
VRRP In:	stances					Export SD-WA Export Netwo
lame	; VRI	D : Interface : VIF	State Priority	: Advertise interval : N	lopreempt : Managem	ent Show Attache

Задать параметры для экземпляра VRRP:

- Имя vCPE5
- VRID 5 (идентификатор экземпляра, должен совпадать у всех устройств VRRP группы).
- Interface lan (сетевой интерфейс, который ассоциируется с VRRP).
- VIP 10.20.5.1/24 (виртуальный IP адрес, который будет назначен основному маршрутизатору группы).
- State MASTER (состояние маршрутизатора, в данном сценарии vCPE-51 будет основным).
- Priority 100 (приоритет маршрутизатора, более высокий приоритет означает, что маршрутизатор будет выбран основным).

Нажать Create.

VRRP instances VRRP groups VRRP Enabled You must create at least one instance	New VRRP instan	ce		×		Actions Delets Import Export Clone
- VKN-Instance	Name vCPE-5 Priority 100 Unicast	VRID ⑦ Interfn 5 Interfn Advertise interval ⑦ 5 Aain VRPP router IP	Acce ⑦ VIP ⑦ 10 20 5.1/24 Nopreempt ⑦ Backup VRRP router IP	State Master 🗸	: Management :	Export network interfaces Show associated CPEs
	Authentication F	essword		Close Croste		

	e nuse PE-51 ormation Multipathing Deactivatie v VRRP Groups v ces i VRID	on Encryption Configurations	SD-WAN Settings 1	Topology NetworkSettings ate <u>i</u> Priority	BGP Settings BFD Settings	Static Routes VI	RRP More *	Close Actions Delete Import Export Clone Export SD-WAN Configuration Export Network Settings
vores , vores	5	lan	10 20 5 1/24 M	ASTER 100	5	No	Edit Remove	Snow Attached OPE



5.2.3. Повторить пункт 5.2.2 для vCPE-52 со следующими параметрами VRRP:

- Имя vCPE5
- VRID 5 (идентификатор экземпляра, должен совпадать у всех устройств VRRP группы).
- Interface lan (сетевой интерфейс, который ассоциируется с VRRP).
- VIP 10.20.5.1/24 (виртуальный IP адрес, который будет назначен основному маршрутизатору группы).
- State BACKUP (состояние маршрутизатора, в данном сценарии vCPE-52 является резервным).
- Priority 50 (приоритет маршрутизатора, более высокий приоритет означает, что маршрутизатор будет выбран основным).
- 5.2.4. Проверка работы экземпляра VRRP.

Подключится к vCPE-51. Для просмотра пароля от CPE выбрать vCPE-51 и нажать Show password.

SD-WAN		+ CPE	+ CPE template + UNI te	emplate + SD-WAN instance ten	mplate + SD-WAN instance pool	+ Firmware + Certificate
	VCPE-51 Configuration Monitoring Problems Encryption Ser	vice requests . Tags Sori	ipts SD-WAN settings Topolog	y . Network settings . BGP settings	OSPF Routing Filters More *	Save Close
÷	VCPE-51 Demolab DPID Customer tenant	CPE templa	te Lt	Juation		Actions Delete Set location
୶ୄୗୄୡୄ	8000005056AAB512 Demolab Description	VCPE-51	~			Deactivate Show password Get activation URL
₽ -						Open SSH console Run scripts Reboot
1	Device information Model SW version Controller	Gateways User R	egistered Update	Management IP State Conne	ection	Shutdown Export SD-WAN settings Export network interfaces
- -	x86_64 VM knaas-cpe_2 23.07 release 23 bios amd64 10.50.114 : 6653	- admin 0	7/11/2023 17:43 14/11/2023 15:14	10.11.12.251 Activated Conne	ected	
2	Out-of-band management Type	Status	Last update	0		
1	Upgrade Network	Completed	14/11/2023 15:04			
	VRRP	Completed	14/11/2023 15:10			

Проверить, что маршрутизатор назначил виртуальный IP-адрес на интерфейс lan.

ip a | grep eth2 -A 3

root@8000005056AAB512:~# ip a grep eth2 -A 3
4: eth2: <broadcast,multicast,up,lower_up> mtu 1500 qdisc mq state UP group default qlen 1000</broadcast,multicast,up,lower_up>
link/ether 00:50:56:aa:dd:49 brd ff:ff:ff:ff:ff:ff
inet 10.20.5.3/24 brd 10.20.5.255 scope global eth2
valid lft forever preferred lft forever
inet 10.20.5.1/24 scope global secondary eth2
valid lft forever preferred lft forever
inet6 fe80::250:56ff:feaa:dd49/64 scope link
valid lft forever preferred lft forever
root@8000005056AAB512:~#

Подключится к хосту wst5 и проверить связность с wst3:

[root@wst5~]\$ ping 10.20.3.11

```
[ivpanin@wst5 ~]$ ping 10.20.3.11
PING 10.20.3.11 (10.20.3.11) 56(84) bytes of data.
64 bytes from 10.20.3.11: icmp_seq=1 ttl=62 time=3.63 ms
64 bytes from 10.20.3.11: icmp_seq=2 ttl=62 time=3.62 ms
64 bytes from 10.20.3.11: icmp seq=3 ttl=62 time=2.93 ms
64 bytes from 10.20.3.11: icmp seq=4 ttl=62 time=3.32 ms
64 bytes from 10.20.3.11: icmp seq=5 ttl=62 time=3.17 ms
64 bytes from 10.20.3.11: icmp seq=6 ttl=62 time=2.17 ms
64 bytes from 10.20.3.11: icmp seq=7 ttl=62 time=2.09 ms
64 bytes from 10.20.3.11: icmp_seq=8 ttl=62 time=3.34 ms
64 bytes from 10.20.3.11: icmp_seq=9 ttl=62 time=3.40 ms
64 bytes from 10.20.3.11: icmp_seq=10 ttl=62 time=3.24 ms
64 bytes from 10.20.3.11: icmp seq=11 ttl=62 time=3.57 ms
64 bytes from 10.20.3.11: icmp seq=12 ttl=62 time=3.48 ms
64 bytes from 10.20.3.11: icmp seq=13 ttl=62 time=3.79 ms
64 bytes from 10.20.3.11: icmp seg=14 ttl=62 time=3.58 ms
```

Отключить lan интерфейс (eth2) на vCPE-51:

ip link set dev eth2 down

Подключится к vCPE-52. Для просмотра пароля от CPE выбрать vCPE-52 и нажать Show password.

Проверить, что данный маршрутизатор назначил виртуальный IP-адрес на lan интерфейс (eth2).

ip a | grep eth2 -A 3

```
root@8000005056AAC6B5:~# ip a | grep eth2 -A 3
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group defa
ult qlen 1000
    link/ether 00:50:56:aa:f1:04 brd ff:ff:ff:ff:ff:ff
    inet 10.20.5.2/24 brd 10.20.5.255 scope global eth2
    valid_lft forever preferred_lft forever
    inet 10.20.5.1/24 scope global secondary eth2
    valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feaa:f104/64 scope link
    valid_lft forever preferred_lft forever
    root@8000005056AAC6B5:~#
```

Подключится к хосту wst5 и проверить связность с wst3:

[root@wst5~]\$ ping 10.20.3.11

[ivpanin@wst5 ~]\$ ping 10.20.3.11					
PING 10.20.3.11 (10.20.3.11) 56(84) bytes of data.					
54 bytes from 10.20.3.11: icmp seq=1 ttl=62 time=2.73 ms					
54 bytes from 10.20.3.11: icmp seq=2 ttl=62 time=3.15 ms					
54 bytes from 10.20.3.11: icmp_seq=3 ttl=62 time=2.91 ms					
54 bytes from 10.20.3.11: icmp_seq=4 ttl=62 time=2.68 ms					
54 bytes from 10.20.3.11: icmp_seq=5 ttl=62 time=2.34 ms					
54 bytes from 10.20.3.11: icmp_seq=6 ttl=62 time=3.08 ms					
54 bytes from 10.20.3.11: icmp_seq=7 ttl=62 time=3.15 ms					
54 bytes from 10.20.3.11: icmp_seq=8 ttl=62 time=2.95 ms					
54 bytes from 10.20.3.11: icmp_seq=9 ttl=62 time=3.48 ms					
54 bytes from 10.20.3.11: icmp_seq=10 ttl=62 time=3.35 ms					
54 bytes from 10.20.3.11: icmp_seq=11 ttl=62 time=3.23 ms					
54 bytes from 10.20.3.11: icmp seq=12 ttl=62 time=3.36 ms					
54 bytes from 10.20.3.11: icmp seq=13 ttl=62 time=3.28 ms					
54 bytes from 10.20.3.11: icmp_seq=14 ttl=62 time=3.10 ms					
54 bytes from 10.20.3.11: icmp seq=15 ttl=62 time=3.26 ms					

Как видно, связность между рабочими станциями сохранилась и VRRP отработал корректно.

5.2.5. Возврат настроек после завершения теста.

Требуется включить интерфейс lan(eth2) на vCPE-51.

Подключиться к vCPE-51 и выполнить:

ip link set dev eth2 up

Проверить, что данный маршрутизатор назначил виртуальный IP-адрес на lan интерфейс (eth2).

ip a | grep eth2 -A 3

```
root@8000005056AAB512:~# ip a | grep eth2 -A 3
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether 00:50:56:aa:dd:49 brd ff:ff:ff:ff:ff
inet 10.20.5.3/24 brd 10.20.5.255 scope global eth2
valid lft forever preferred lft forever
inet 10.20.5.1/24 scope global secondary eth2
valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:feaa:dd49/64 scope link
valid_lft forever preferred_lft forever
root@8000005056AAB512:~#
```

Приложение А.

Checklist.

Перед выполнением тестов должны быть выполнены все настройки из документа Proof of Concept Руководство по настройке демонстрационного стенда Kaspersky SD-WAN 2.0 Часть 1.

Ν	Название теста	Пункт настр ойки	Ожидаемый результат	Результа т проверки (пройден /не пройден)
1	Управление трафиком.			
1.1	Балансировка нагрузки в режиме Active / Active.	3.1	Трафик балансируется между двумя WAN интерфейсами устройства vCPE-3.	
1.2	Резервирование каналов связи в режиме Active/Standby.	3.2	При работающем основном WAN интерфейсе устройства vCPE-3 трафик не идет через резервный WAN интерфейс. При отключении основного WAN- интерфейса на устройстве vCPE-3 трафик переключается на резервный WAN- интерфейс.	
1.3	Резервирование каналов связи в широковещательном (broadcast) режиме.	3.3	Копии пакетов с устройства vCPE-3 отправляются по интерфейсам genev_sys_4800/4801 в сторону vGW- 11/12.	
1.4	Использование механизма FEC.	3.4	При включении FEC уменьшается процент потерь пакетов на интерфейсе, для которого включена эмуляция потерь.	
1.5	Включение мониторинга потерь пакетов на туннелях.	3.4.2- 3.4.4	При включении мониторинга потерь в оркестраторе отображается статистика потерь для туннелей.	
1.6	Включение мониторинга задержек и джиттера на туннелях.	3.5.2- 3.5.7	При включении мониторинга задержек и джиттера в оркестраторе отображается статистика задержек и джиттера для туннелей.	
1.7	Управление трафиком с помощью ограничений (Constraints).	3.5	При применении ограничений на транспортный сервис из пути прохождения трафика исключаются туннели, не удовлетворяющие заданным условиям (задаются пороговые значения задержки и джиттера). В статистике iperf уменьшается значения джиттера для	

			трафика, проходящего от устройства vCPE-3 к vCPE-4.	
1.8	Классификация трафика с помощью ACL и перенаправления в туннели, соответствующих заданным ограничениями.	3.6	Трафик, подпадающий под параметры созданного ACL (protocol UDP, port 5555), перенаправляется в туннели, не отмеченные как "Unsolicited".	
1.9	Классификация трафика с помощью DPI и перенаправления в туннели, соответствующие заданным ограничениями.	3.7	Трафик, подпадающий под параметры созданного DPI ACL (SSH и HTTP), перенаправляется в туннели, не отмеченные как " Unsolicited ".	

2	Построение топологии SD-WAN сети.			
2.1	Создание топологий Full-Mesh.	4.1	После настройки топологических тегов, устройства СРЕ создают дополнительные туннели для построения Full-Mesh топологии (от каждого устройства СРЕ созданы туннели до всех других устройств СРЕ).	
2.2	Создание топологий Partial-Mesh.	4.2	После настройки топологических тегов, устройства СРЕ создают дополнительные туннели для построения Partial-Mesh топологии. Созданы 2 группы СРЕ: vCPE- 3 и vCPE-4, и vCPE-51, vCPE-52, vCPE-4. СРЕ данных группы строят прямые туннели до всех устройств в своей группе.	
2.3	Создание топологий с использованием транзитных СРЕ.	4.3	Устройства vCPE-3 и vCPE-51 строят туннели через устройство vCPE-4, отмеченное как транзитное.	

3	Работа с СРЕ устройствами.			
3.1	Централизованное обновление firmware CPE устройств.	5.1	Firmware успешно загружено в оркестратор. Для СРЕ отображается доступность новой версии firmware. Обновление СРЕ на новую версию firmware проходит успешно: СРЕ после загрузки успешно подключаются к контроллеру и в интерфейсе оркестратора отображается новая версия firmware.	
3.2	Резервирование устройств СРЕ с использованием VRRP.	5.2	На паре устройств vCPE-51/52 успешно применяются настройки VRRP. На VRRP Master (vCPE-51) появляется настроенный виртуальный IP и обеспечивается связность между хостами wst5 и srv1. При отключении lan интерфейса на vCPE-51, виртуальный IP адрес переходит на устройство vCPE-52, которое становится VRRP Master, при этом также обеспечивается связность между хостами wst5 и srv1.	



https://kaspersky.ru/ https://securelist.ru

© 2023 АО «Лаборатория Касперского»