Kaspersky SD-WAN

Proof of Concept

18.12.2024

Версия документа:
2.3.1.0

Руководство по развертыванию демонстрационного стенда
Часть 2: настройка сценариев классификации, приоритезации и управления трафиком, построения Full-Mesh и Partial-Mesh топологий

kaspersky активируй будущее

Центр экспертизы
по корпоративным решениям

kaspersky

Изменения

Дата	Изменения
05.07.2023	Первая версия документа.
19.07.2023	Исправлены ошибки, добавлен сценарий VRRP, добавлен сценарий дублирования пакетов, добавлен сценарий FEC.
27.07.2023	Исправлены ошибки, обновлено описание сценариев.
28.07.2023	Добавлен чеклист
02.08.2023	Документ обновлен по релизу Kaspersky SD-WAN 2.3.1.
22.08.2023	Описание сценариев обновлено по полученной обратной связи.
14.11.2023	Документ обновлен по релизу Kaspersky SD-WAN 2.3.1.
24.05.2024	Документ обновлен по релизу Kaspersky SD-WAN 2.2.1. Убрана секция VRRP (перенесена в PoC часть 1). Убрана секция обновления CPE (перенесена в CPE maintenance guide).
24.05.2024	Документ обновлен по релизу Kaspersky SD-WAN 2.2.1. Убрана секция VRRP (перенесена в PoC часть 1). Убрана секция обновления CPE (перенесена в CPE maintenance guide).
18.12.2024	Документ обновлен по релизу Kaspersky SD-WAN 2.3.1.

kaspersky

Содержание

kaspersky

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 различного типа.
- Использование несколько виртуальных каналов для обеспечения высокой доступности сети и балансировки трафика.
- Коррекция ошибок при передаче данных.
- Интеллектуальное управление трафиком.
- Легкая настройка устройств CPE с использованием Configuration URL.
- 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 устройств CPE.
- SD-WAN контроллер. Управляет наложенной сетью (англ. Overlay Network), обеспечивает построение топологии сети и создание транспортных сервисов внутри наложенных линков. Поддерживает транспортные сервисы L2 Point-to-Point (P2P), Point-to-Multipoint (P2M), Multipoint-to-Multipoint (M2M) и L3 VPN. Управляет устройствами CPE и шлюзами SD-WAN по протоколу OpenFlow. Определяет распределение трафика между линками, выполняет мониторинг качества соединения и автоматическое переключение трафика на резервный линк в случае возникновения проблем на основном. Контроллер находится под управлением SD-WAN оркестратора.
- SD-WAN шлюзы. Объединяют устройства CPE в единую сеть. Наложенные линки терминируются на SD-WAN шлюзах, после чего трафик передается дальше в соответствии с топологией сети.
- CPE устройства или Kaspersky Edge Service Router (KESR). Телекоммуникационное оборудование, которое подключается к шлюзам SD-WAN с помощью наложенных линков и образует SDN-фабрику в виде наложенной сети.

Архитектура решения Kaspersky SD-WAN представлена на рисунке 1.

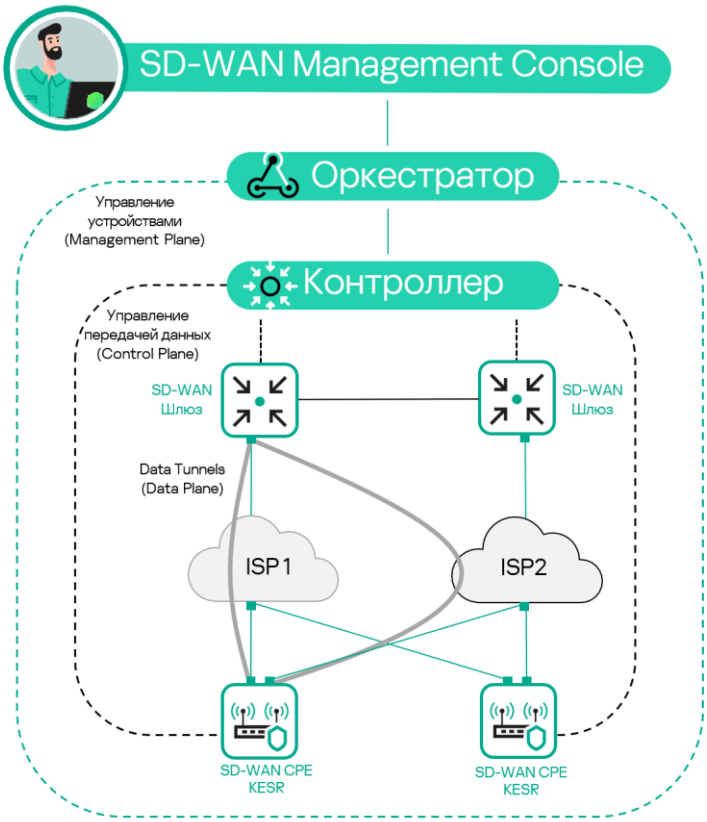


Рисунок 1 - Архитектура решения Kaspersky SD-WAN

kaspersky

2. **Описание схемы демонстрационного стенда Kaspersky SD-WAN**

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

На виртуальном хосте orc1 развернуты Docker контейнеры решения Kaspersky SD-WAN, включая оркестратор, контроллер 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 Source Network Address Translation (SNAT) для vGW-11 и vGW-12 и Destination Network Address Translation (DNAT) для портов, указанных в таблице 2
- 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 2 для Docker контейнеров SD-WAN оркестратора и SD-WAN контроллера.
- Хост ISP эмулирует подключение к сети Интернет / операторам связи ISP1 – ISP8.
- Для подключения устройств CPE SD-WAN шлюзы должны быть доступны по определённому набору портов, перечисленных в таблице 2.
- Устройство vCPE-3 представляет собой пример подключения удаленной площадки с одним устройством CPE, 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.
- Устройства vCPE-51 и vCPE-52 представляют собой пример подключения удаленной площадки с двумя устройствами CPE с использованием протокола VRRP.

2.1. **Схема демонстрационного стенда**

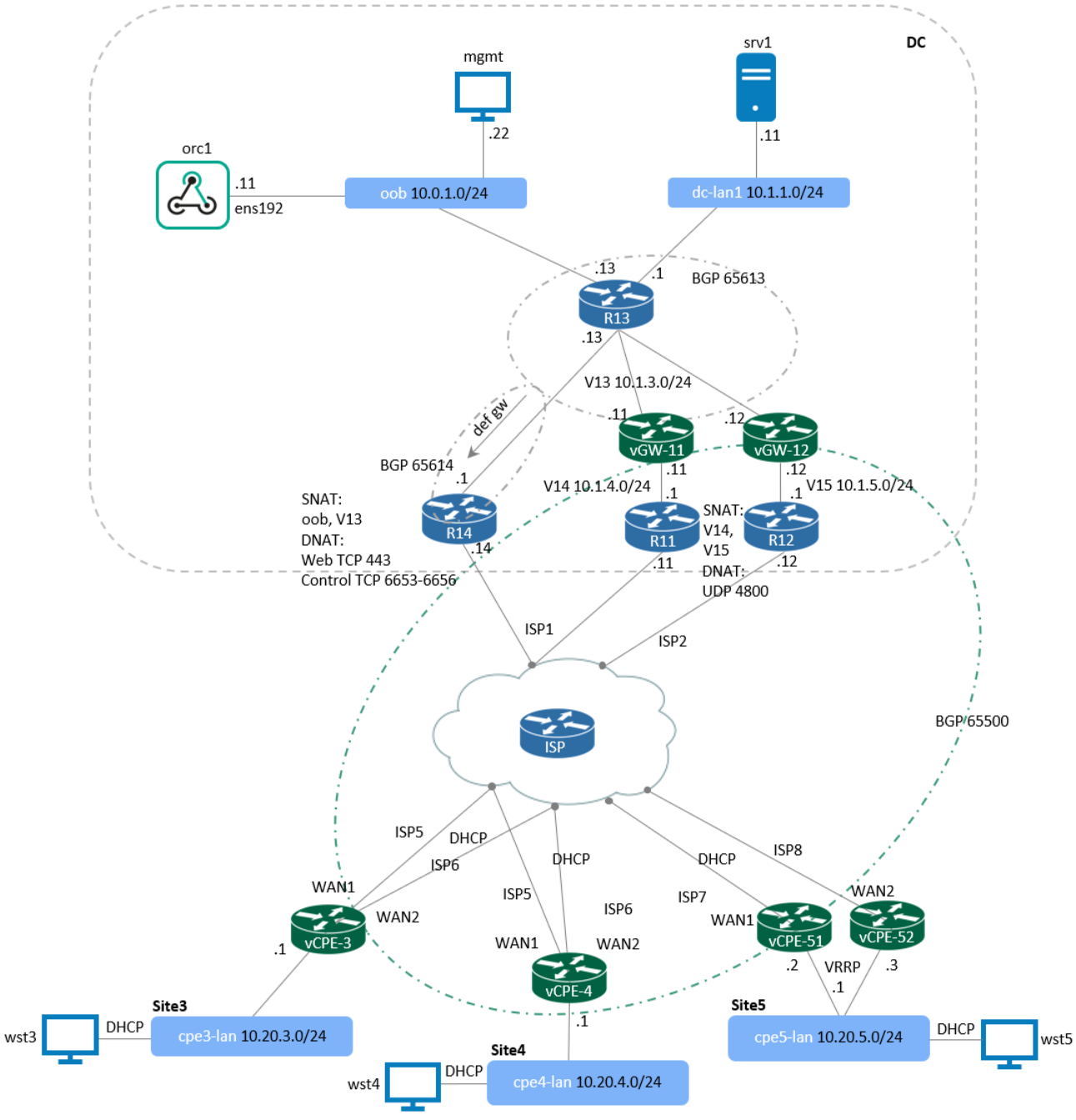


Рисунок 2 - Демонстрационный стенд Kaspersky SD-WAN

2.2. План IP-адресации и требуемые ресурсы для компонентов SD-WAN

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

Таблица 1 – Параметры хостов, используемых в PoC

Имя	Операционная система	IP-адрес	Назначение	Требуемые ресурсы
orc1	Ubuntu 22.04.06 LTS Server	10.0.1.11	На хосте развернуты Docker контейнеры: www-1, orc-1, redis-1m, mongo-1, vnfm-1, vnfm-proxy-1, ctl-1, zabbix-www-1, zabbix-srv-1, zabbix-proxy-1, zabbix-db-1, syslog-1, mockpnf-1	24 x vCPU, 24 GB RAM
vGW-11	Образ vKESR-M2	wan 10.1.4.11 lan 10.1.3.11	SD-WAN шлюз	4 x vCPU, 8 GB RAM
vGW-12	Образ vKESR-M2	wan 10.1.5.12 lan 10.1.3.12	SD-WAN шлюз	4 x vCPU, 8 GB RAM
vCPE-3	Образ vKESR-M1	wan DHCP lan 10.20.3.1	CPE	2 x vCPU, 512 Mb RAM
vCPE-4	Образ vKESR-M1	wan DHCP lan 10.20.4.1	CPE	2 x vCPU, 512 Mb RAM
vCPE-51	Образ vKESR-M1	wan DHCP lan 10.20.5.2 / vIP 10.20.5.1	CPE	2 x vCPU, 512 Mb RAM
vCPE-52	Образ vKESR-M1	wan DHCP lan 10.20.5.3 / vIP 10.20.5.1	CPE	2 x vCPU, 512 Mb RAM
R11	CentOS 7	wan 10.50.1.11 lan 10.1.4.1	Пограничный маршрутизатор DC	2 x vCPU, 2 GB RAM

Имя	Операционная система	IP-адрес	Назначение	Требуемые ресурсы
R12	CentOS 7	wan 10.50.2.12 lan 10.1.5.1	Пограничный маршрутизатор DC	2 x vCPU, 2 GB RAM
R13	CentOS 7	dc-perim 10.1.3.13 oob 10.0.1.13 dc-lan1 10.1.1.1	Маршрутизатор ядра DC	2 x vCPU, 2 GB RAM
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	DHCP 10.20.3.0/24	Рабочая станция Site3	2 x vCPU, 4 GB RAM
wst4	CentOS 7	DHCP 10.20.4.0/24	Рабочая станция Site4	2 x vCPU, 4 GB RAM
wst5	CentOS 7	DHCP 10.20.5.0/24	Рабочая станция Site5	2 x vCPU, 4 GB RAM
mgmt	Windows Server 2022	10.0.1.22 10.1.1.22 10.1.3.22 10.50.1.22 10.20.3.22 10.20.4.22 10.20.5.22	Рабочая станция для управления демо стендом.	6 x vCPU, 6 GB RAM

2.3. **Сетевые порты, используемые компонентами решения**

В таблице 2 представлены сетевые порты, используемые для взаимодействия SD-WAN шлюзов и устройств CPE с центральными компонентами решения, и доступа к веб-интерфейсу оркестратора для администрирования.

Таблица 2 - Сетевые порты, используемые для взаимодействия с решением SD-WAN.

Компонент	**Порт**	**Назначение**
SD-WAN оркестратор	TCP 443 / TLS	Доступ к веб-интерфейсу оркестратора и подключение CPE к оркестратору
SD-WAN контроллер	TCP 6653-6656 / TLS	Подключение SD-WAN шлюзов и устройств CPE к контроллеру. CPE устройство подключается каждым WAN интерфейсом к отдельному порту контроллера: • sdwan0 - 6653 • sdwan1 - 6654 • и т.д.
Zabbix	TCP 85 / TLS TCP10051 / TLS	Доступ к веб- интерфейсу Zabbix. Подключение агентов мониторинга Zabbix с CPE к системе мониторинга
SD-WAN шлюзы	UDP 4800-4803	Дата трафик

2.4. **Схема внешних соединений контейнеров SD-WAN на хосте orc1**

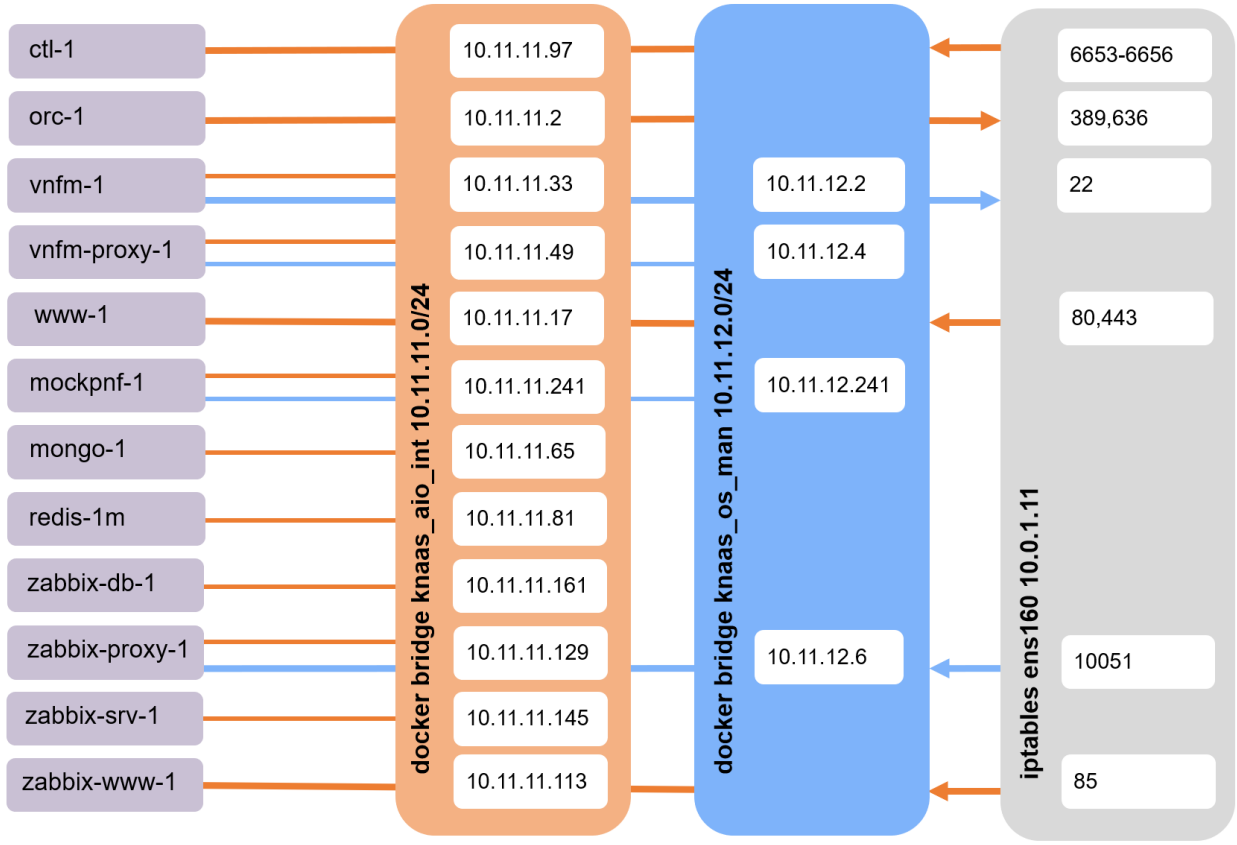


Рисунок 3 - Схема внешних соединений контейнеров SD-WAN.

Контейнеры SD-WAN разворачиваются на хосте orc1. В процессе установки создаются две сети docker: knaas_aio_int (10.11.11.0/24) и knaas_os_man (10.11.12.0/24).

Сеть knaas_aio_int является основной сетью и предназначена для взаимодействия между контейнерами, а также для связи с внешними хостами.

Сеть knaas_os_man предназначена для связи между центральными компонентами решения и CPE с целью управления и мониторинга.

Плейбуками установки решения SD-WAN будут настроены правила iptables: в цепочку DOCKER_USER добавляются правила, разрешающие следующие TCP соединения:

- Для контейнера ctl-1 входящие по портам 6653-6656 (TLS подключения от CPE к контроллеру).
- Для контейнера orc-1 исходящие по портам 389,636 (LDAP/LDAPS подключения к LDAP серверу).
- Для контейнера vnfm-1 исходящие по порту 22 (SSH консоль до CPE из интерфейса оркестратора SD-WAN).
- Для контейнера www-1 входящие по портам 80 и 443 (HTTPS/TLS подключение к web-интерфейсу оркестратора).
- Для контейнера zabbix-proxy-1 входящие по порту 10051 (мониторинг CPE).
- Для контейнера zabbix-www-1 входящие по порту 85 (HTTPS/TLS подключение к web-интерфейсу системы мониторинга Zabbix).

2.5. **Версии программного обеспечения**

Таблица 3 - Версии программного обеспечения Kaspersky SD-WAN, используемого в данном демонстрационном стенде

Компонент SD-WAN	**Версия**
www	knaas-www:2.24.09.release.65.amd64_en-US_ru-RU
orc	knaas-orc:2.24.09.release.76.amd64_en-US_ru-RU
mongo	mongo:5.0.7.amd64
ctl	knaas-ctl:2.24.09.release.25.amd64_en-US_ru-RU
vnfm	knaas-vnfm:2.24.09.release.15.amd64_en-US_ru-RU
vnfm-proxy	knaas-vnfm-proxy:2.24.09.release.6.amd64_en-US_ru-RU
redis	redis:6.2.7.amd64
zabbix-www	zabbix-web-nginx-mysql:6.0.23.amd64
zabbix-proxy	zabbix-proxy:6.0.23.amd64
zabbix-srv	zabbix-server:6.0.23.amd64
zabbix-db	mariadb-ha:11.1.6.amd64
syslog	syslog-ng:3.30.1.amd64
vCPE	knaas-cpe_2.24.09.release.28
mockpnf	mockpnf: 2.23.09.amd64
Хост orc1	Ubuntu 22.04.05 LTS Server
installer	knaas-installer_2.24.09.release.33.amd64_russia_en-US_ru-RU

2.6. **Требования к аппаратным ресурсам решения Kaspersky SD-WAN**

Таблица 4 - Требования к аппаратным ресурсам для управления до 50 устройств CPE

Хост	**CPU**	**RAM, GB**	**Disk, GB, SSD**
orc1	16 cores / 16 vCPU (HT disabled) / 32 vCPU (HT enabled)	32	50 используется в PoC / 256 рекомендуется

Более подробную информацию об аппаратных требованиях можно получить в Kaspersky SD-WAN Online Help: https://support.kaspersky.com/help/SD-WAN/2.3/ru-RU/239105.htm

3. **Управление трафиком**

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

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

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

- Auto-SPF (Shortest-Path Forwarding). Автоматически рассчитываемый контроллером SD-WAN транспортный путь. Транспортные пути этого типа невозможно 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 линков, через которые транспортный путь будет проходить от устройства CPE в начале сегмента до устройства CPE в конце сегмента.
- Auto-TE. Автоматически рассчитываемый контроллером SD-WAN транспортный путь, учитывающий преднастроенные ограничения (англ. constraints). Ограничениями могут быть значения показателей мониторинга на линках, например, показатель уровня загрузки линка.

Транспортные пути имеют следующие параметры:

- Стоимость (англ. Cost). По умолчанию, является суммой стоимости всех линков, которые входят в транспортный путь. Поддерживается возможность ручного определения стоимости транспортных путей.
- Административное состояние (Administrative state). Задается вручную. Если этот параметр имеет значение down, транспортный путь не используется.
- Фактическое состояние (англ. Operational 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: https://support.kaspersky.com/help/SD-WAN/2.3/ru-RU/250984.htm

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.

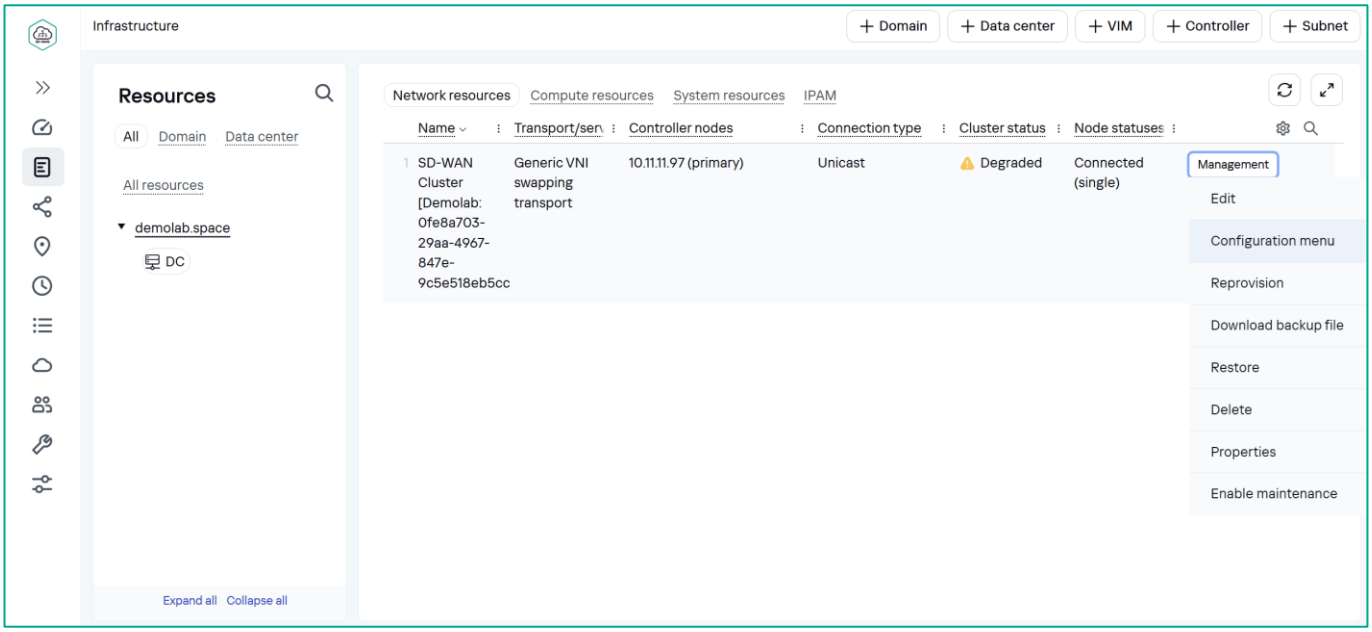
Для получения дополнительной информации о резервировании каналов связи обратитесь к Kaspersky SD-WAN Online Help: https://support.kaspersky.com/help/SD-WAN/2.3/ru-RU/250984.htm

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

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. Просмотреть построенные сегменты SD-WAN.

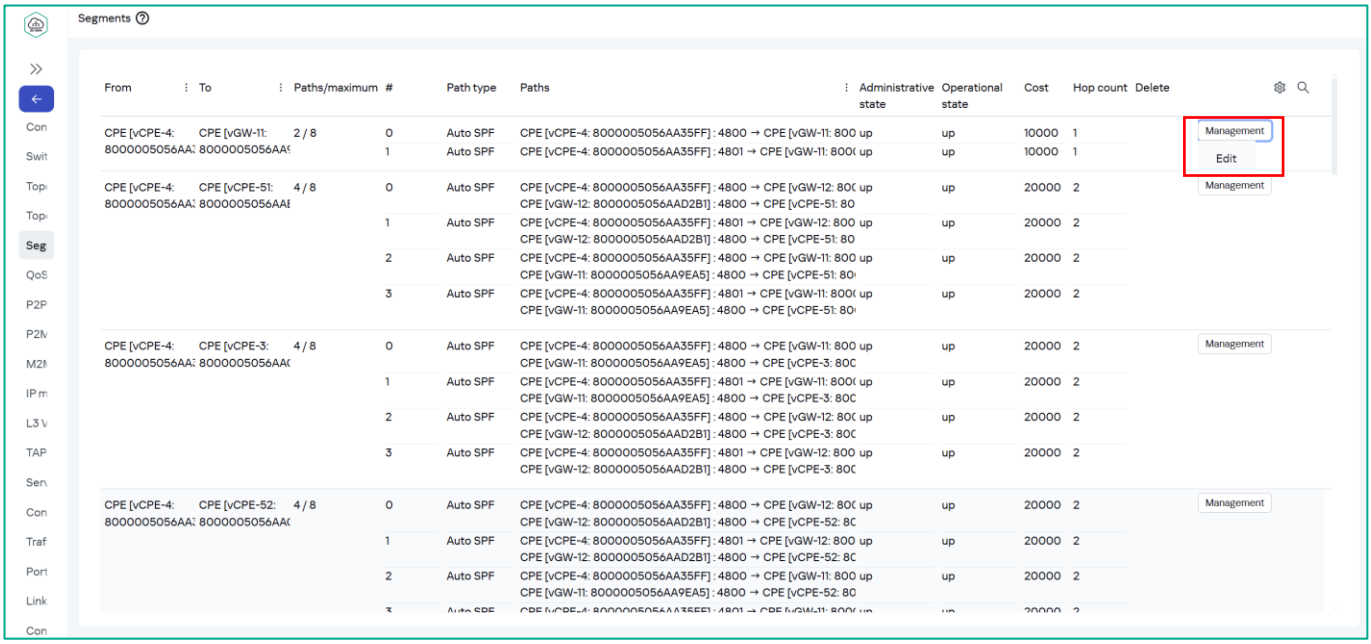
Для отображения перечня всех сегментов SD-WAN перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu → Segments**

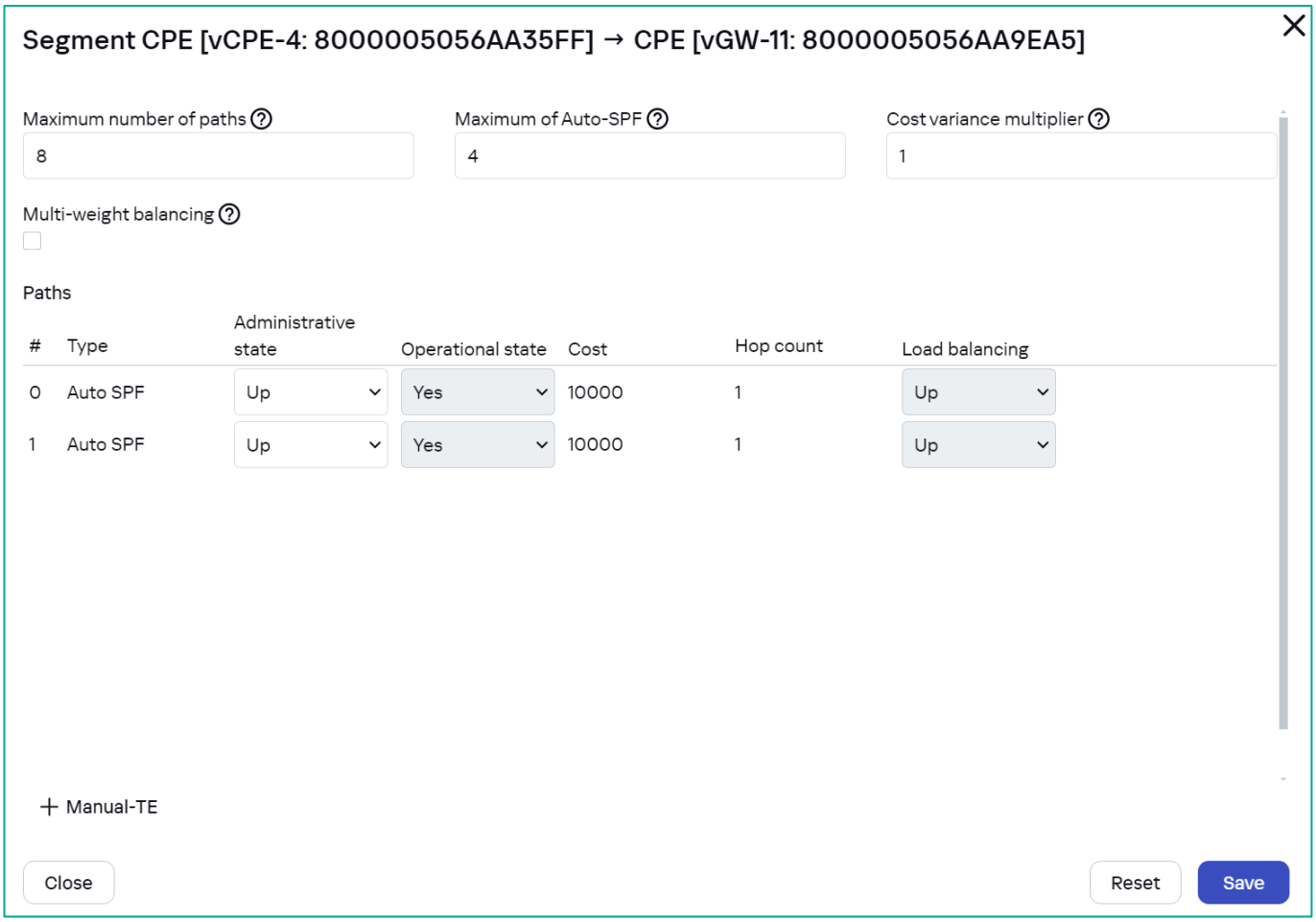


На скриншоте ниже представлены сегменты, построенные между CPE. Все сегменты проходят через CPE с ролью Gateway: vGW-11 и vGW-12. Количество автоматически построенных путей равно 2, в соответствии с настройкой, заданной в шаблоне CPE.

Балансировка между путями осуществляется средствами протокола OpenFlow (группы типа Select).

Для получения дополнительной информации о параметрах сегмента нажать кнопку **Management → Edit**





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 линка (туннеля) между CPE устройствами, линк будет удален из топологии, а трафик перенаправлен на резервный транспортный путь.

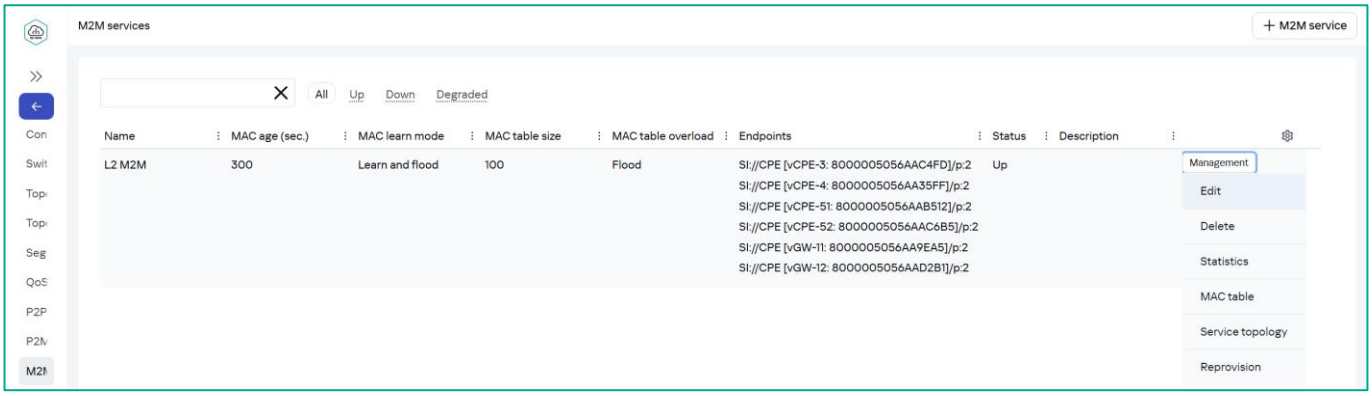
3.1.2. Включить режим балансировки per-packet для транспортного сервиса M2M.

Для транспортных сервисов доступны следующие режимы балансировки:

- Per-flow. Балансировка по потокам. При отправке потоки распределяются равномерно по линкам.
- Per-packet. Балансировка по пакетам. При отправке пакеты распределяются равномерно по линкам.
- Broadcast. Копии пакетов передаются одновременно во все линки для исключения потерь.

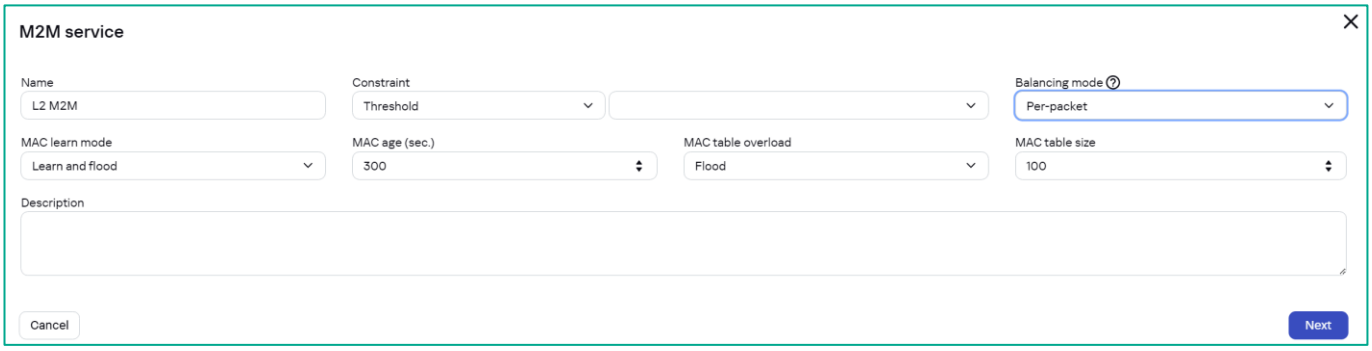
Выбор режима балансировки происходит в настройках транспортного сервиса.

Перейти в меню **M2M services**. Выбрать транспортный сервис **L2 M2M** и нажать **Management → Edit**



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

Задать **Balancing mode**: **Per-packet**

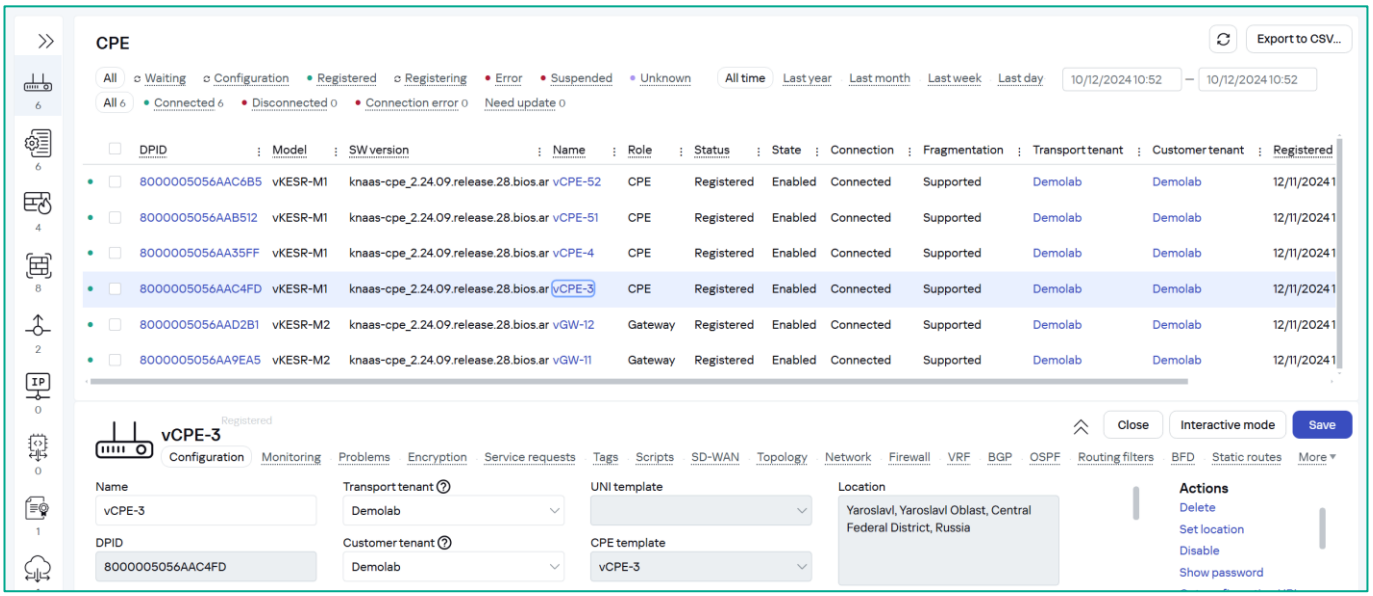


Затем сохранить настройки сервиса: нажать **Next**, **Next** и **Save**

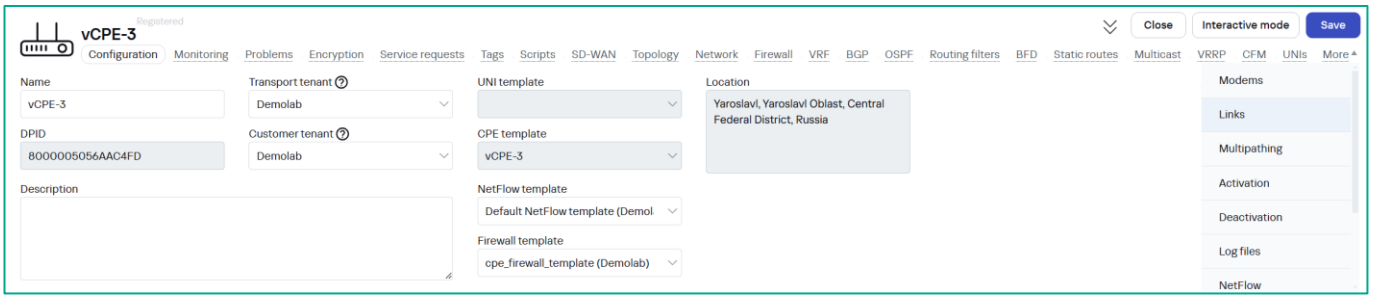
Для получения справочной информации о режимах балансировки обратитесь к Kaspersky SD-WAN Online Help: https://support.kaspersky.com/help/SD-WAN/2.3/ru-RU/245696.htm

3.1.3. Проверить стоимость для линков, построенных vCPE-3.

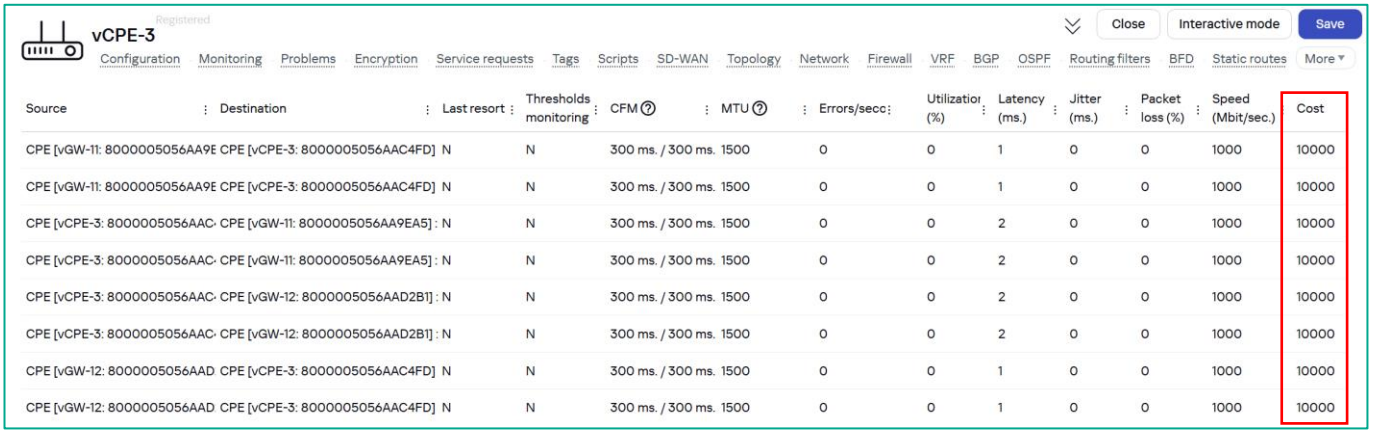
Перейти в меню **CPE** и выбрать **vCPE-3**.



Перейти на вкладку **Links**



Отобразится список построенных линков с **vCPE-3**. В данном сценарии балансировка будет производится между линками с одинаковой стоимостью. Значение стоимости отображается в столбце **Cost** вкладки **Links**. Проверить значение стоимости линков: для работы балансировки быть одинаковое значение стоимости.

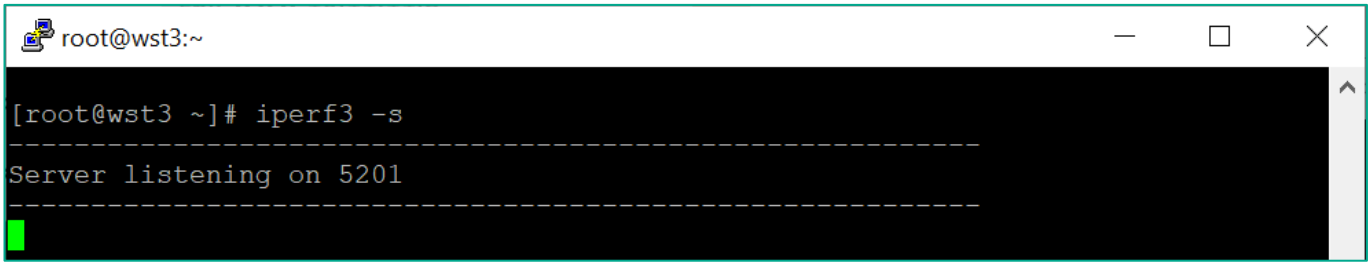


3.1.4. Сгенерировать тестовый трафик между wst3 и wst4.

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

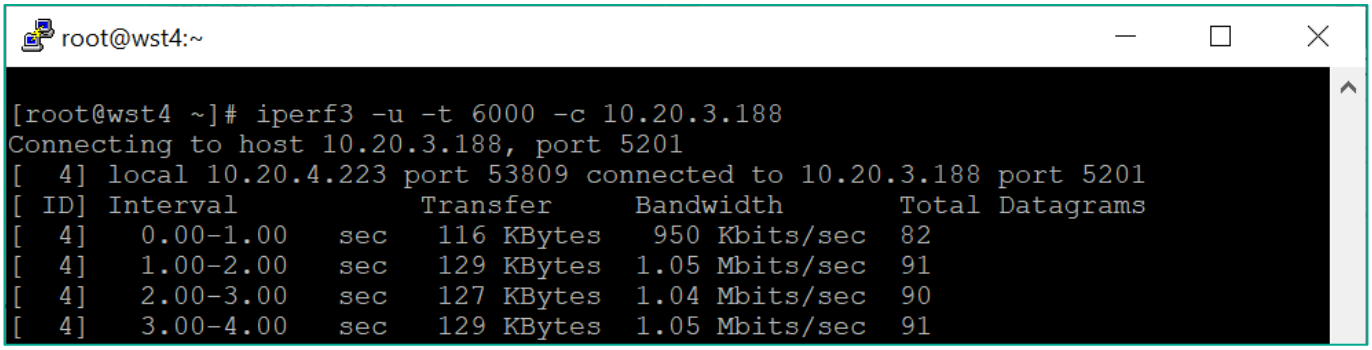
Запустить сервер **iperf** на рабочей станции **wst3**:

```
iperf3 -s
```



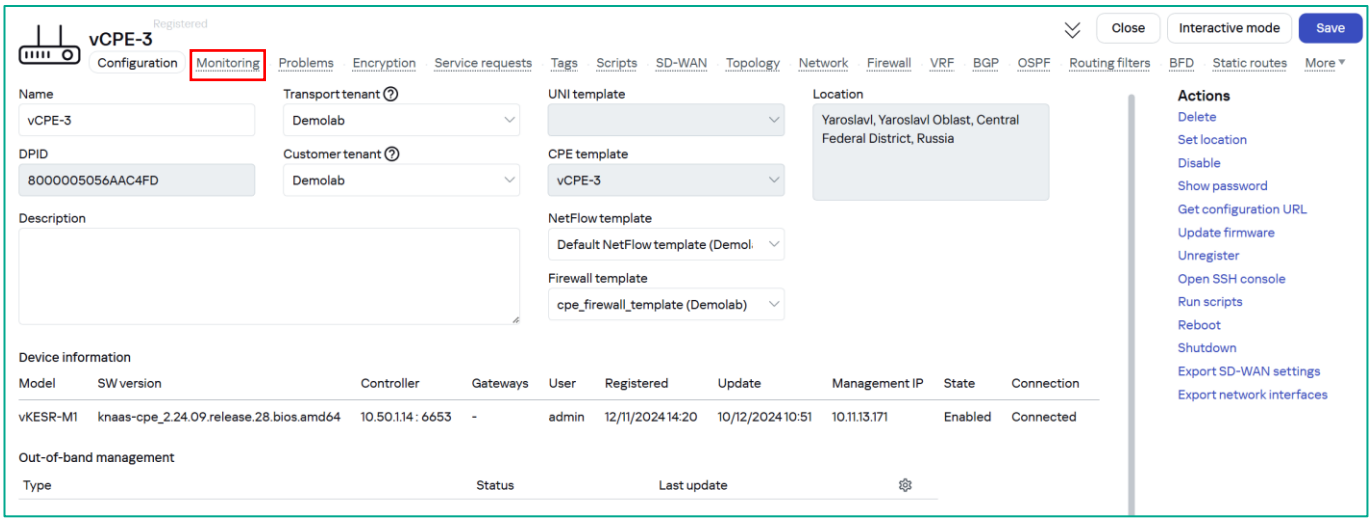
Запустить клиент **iperf** на рабочей станции **wst4** (также необходимо проверить IP адреса, выданные **wst3** и **wst4** – выполнить `ip a` на рабочих станциях):

```
iperf3 -u -t 6000 -c <wst3 IP>
```

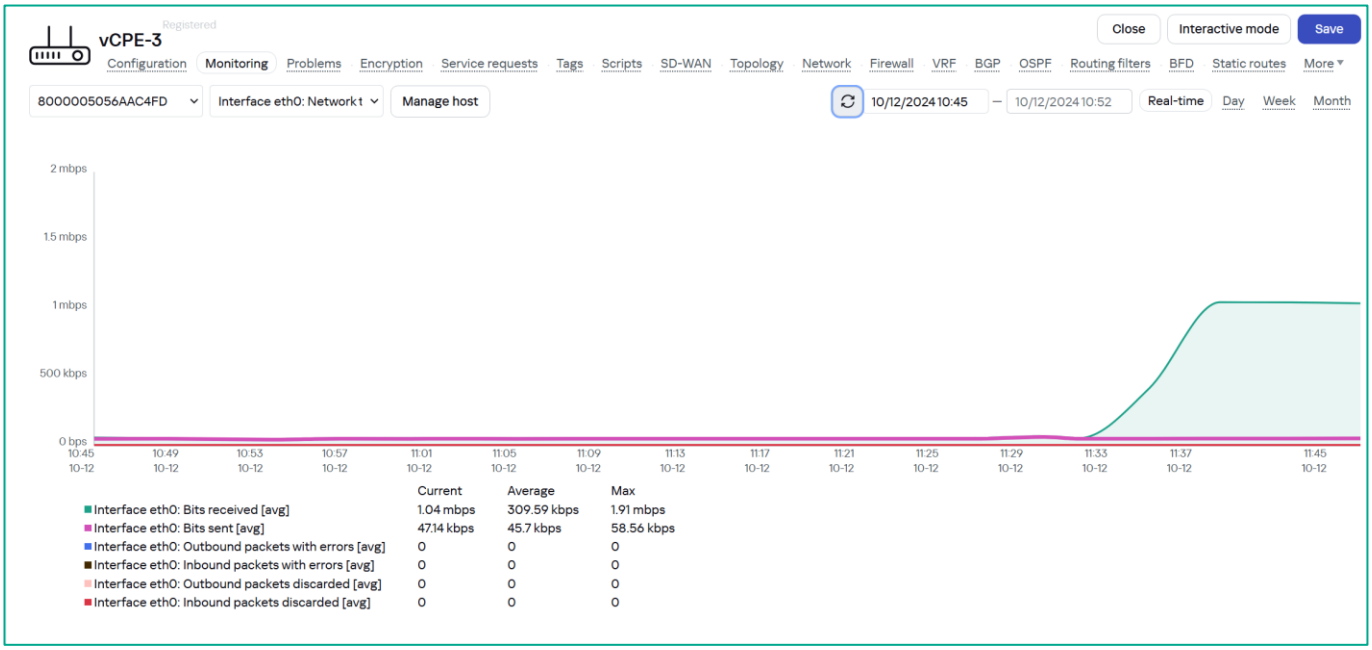


3.1.5. Проверить балансировку трафика между WAN интерфейсами vCPE-3.

Перейти в меню **CPE**, открыть **vCPE-3**, затем открыть вкладку **Monitoring**

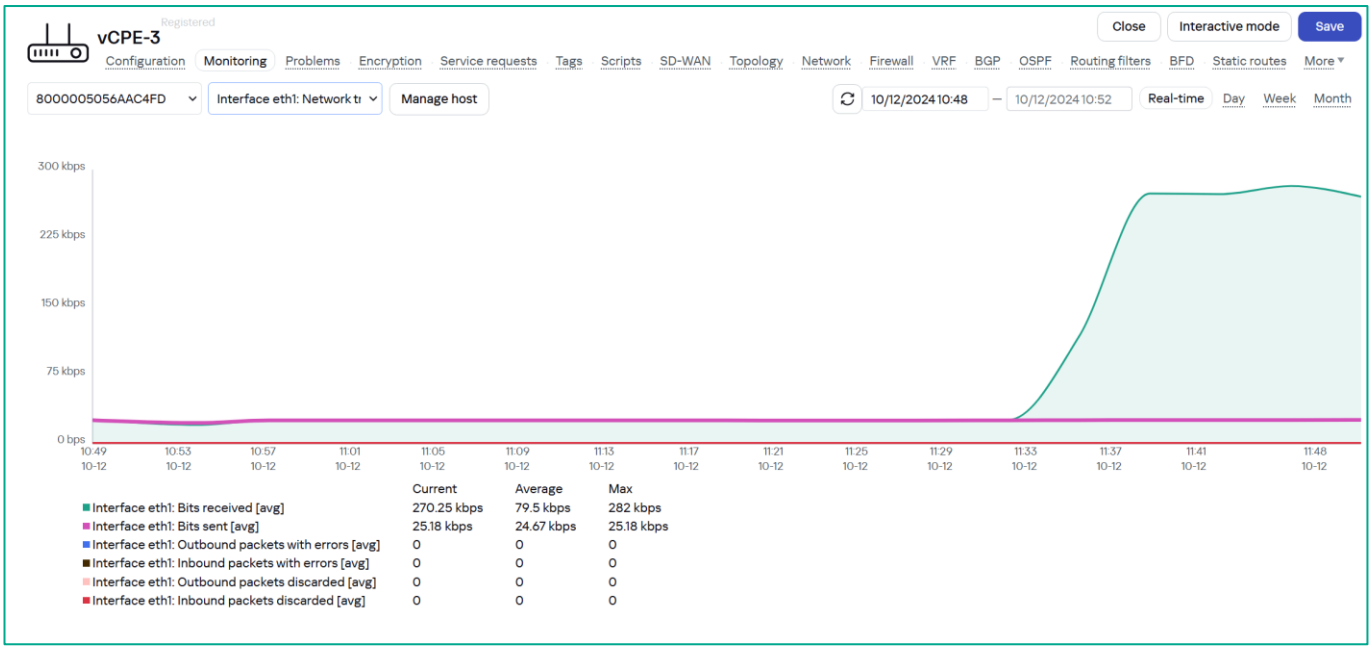


Выбрать **Interface eth0** (интерфейс CPE sdwan0) и убедится на графике, что трафик проходит именно через него – виден всплеск на графике **Interface eth0: Bit received [avg].** Для отображения данных необходимо подождать накопления статистики в течении 10 минут.



Проверить прохождение трафика через второй WAN интерфейс CPE.

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



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

3.1.6. Вернуть настройки после завершения теста

Повторить п. 3.1.2 и изменить режим балансировки на **per-flow**.

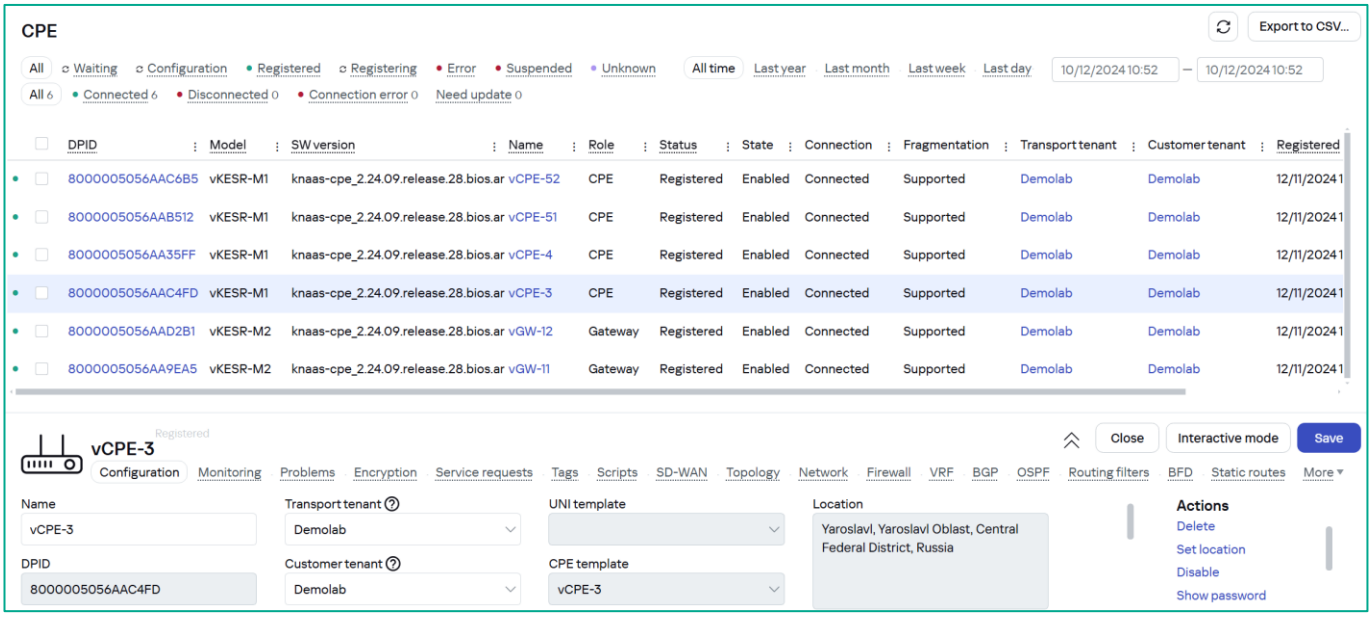
Остановить процессы **iperf** на **wst3** и **wst4**, запущенные в пункте 3.1.4 (возможно прервать с помощью **`Ctrl+Z`**).

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 линке 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.

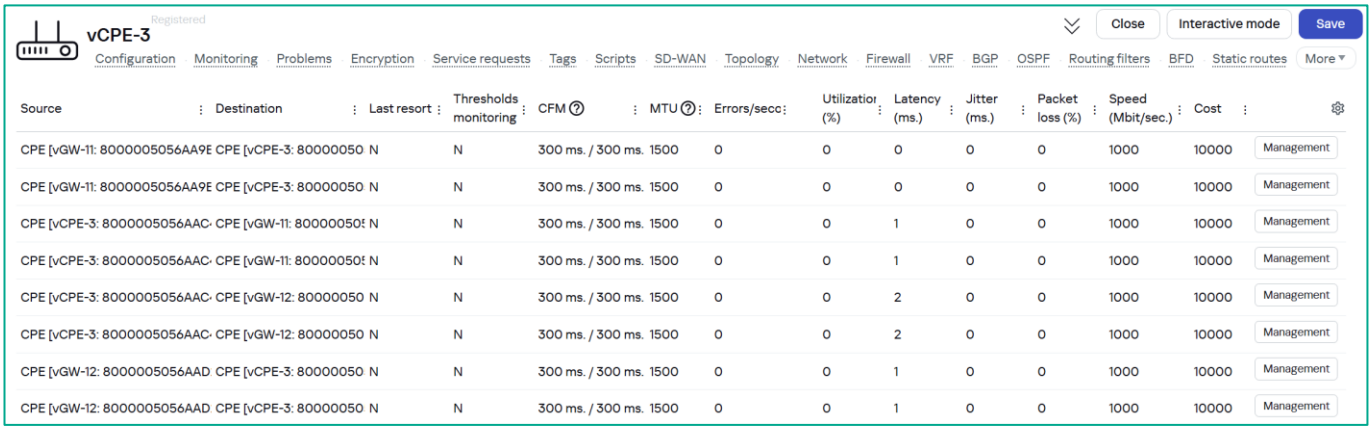
3.2.1. Задать параметры стоимости для резервных линков.

Перейти в меню **CPE** и выбрать **vCPE-3**.



Перейти на вкладку **Links**

На вкладке **Links** представлен список построенных линков выбранного устройства CPE со смежными устройствами. В столбцах **Source** и **Destination** указаны устройства CPE источника и назначения однонаправленного линка. Номер порта указывает на номер WAN интерфейса устройства CPE. 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) и т.д.



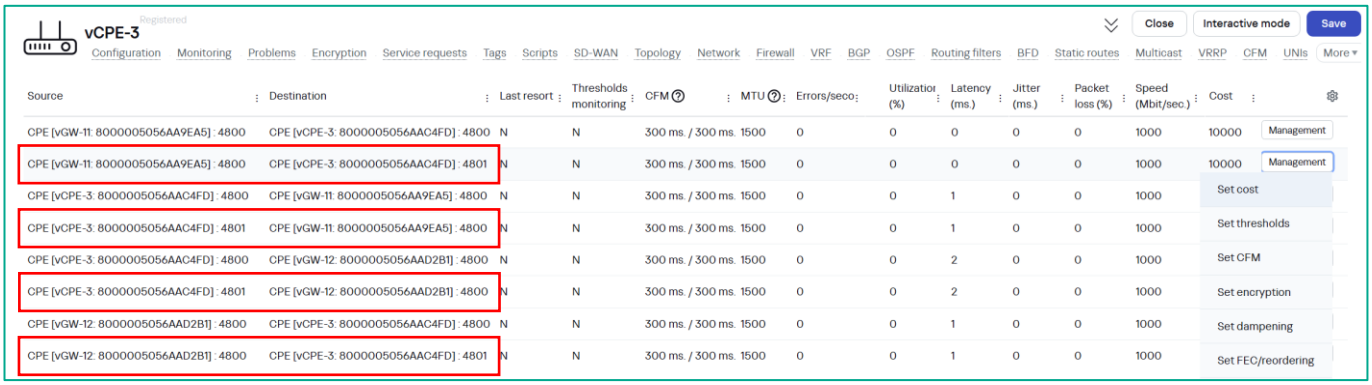
В решении SD-WAN топологией по умолчанию является Hub-and-Spoke, поэтому весь трафик между CPE проходит через шлюзы. В данном сценарии будет увеличена стоимость линков, проходящих через резервный WAN-интерфейс (**sdwan1** / **eth1**) **vCPE-3**, между **vCPE-3** и шлюзами **vGW-11** / **vGW-12**.

Найти все линки 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**

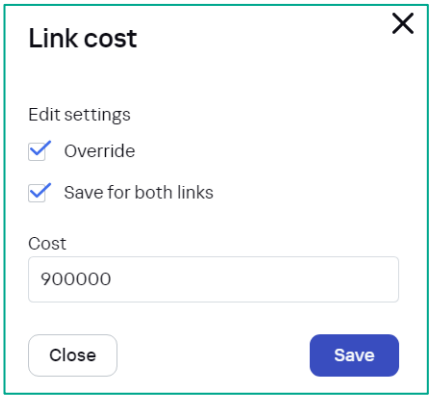
Поочередно для найденных линков изменить стоимость (по умолчанию стоимость зависит от значения **Maximum rate** интерфейсов SD-WAN, в PoC 1000).

Нажать **Management → Set cost**



Задать параметры стоимости линков:

- **Override** - переопределить значение стоимости
- **Cost**: **900000**
- **Save for both links** - применить настройки к обоим линкам между парой CPE устройств



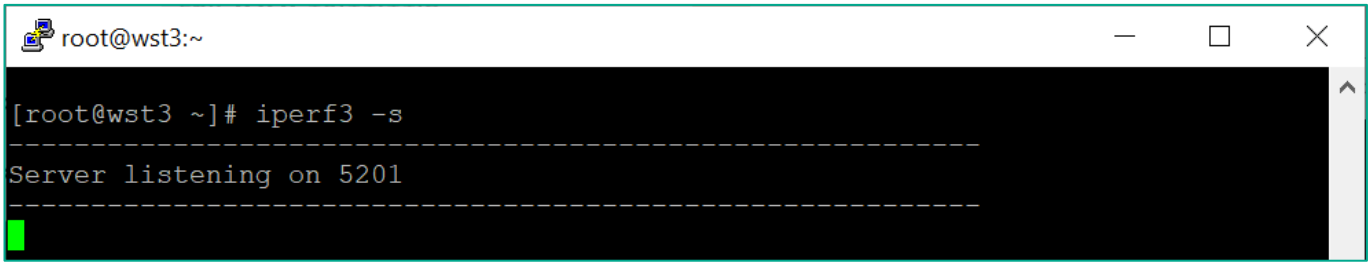
Note: Возможно влиять на стоимость линков посредством изменения значения **Maximum rate** в настройках интерфейсов SD-WAN. Но это же значение также влияет и на шейпер, настраиваемый для исходящего трафика SD-WAN интерфейсов.

3.2.2. Сгенерировать тестовый трафик между wst3 и wst4.

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

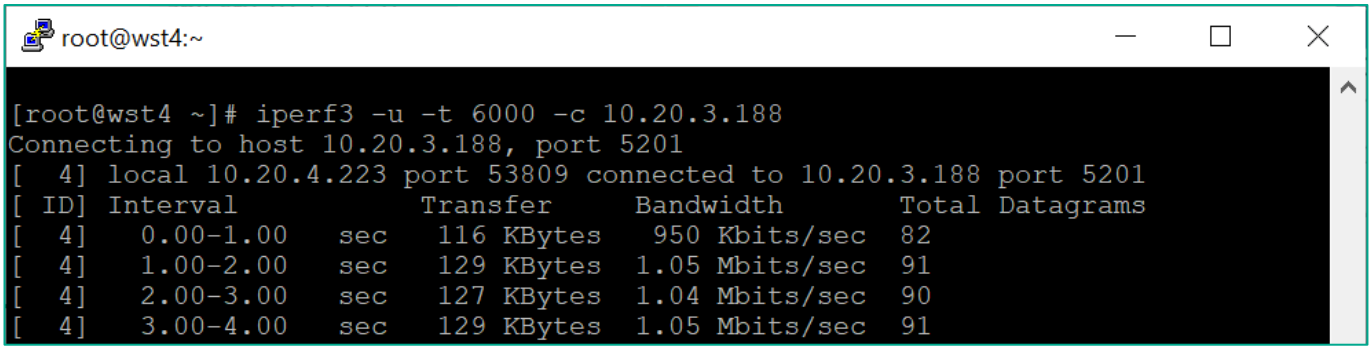
Запустить сервер **iperf** на рабочей станции **wst3**:

```
iperf3 -s
```



Запустить клиент **iperf** на рабочей станции **wst4** (также необходимо проверить IP адреса, выданные **wst3** и **wst4** – выполнить `ip a` на рабочих станциях):

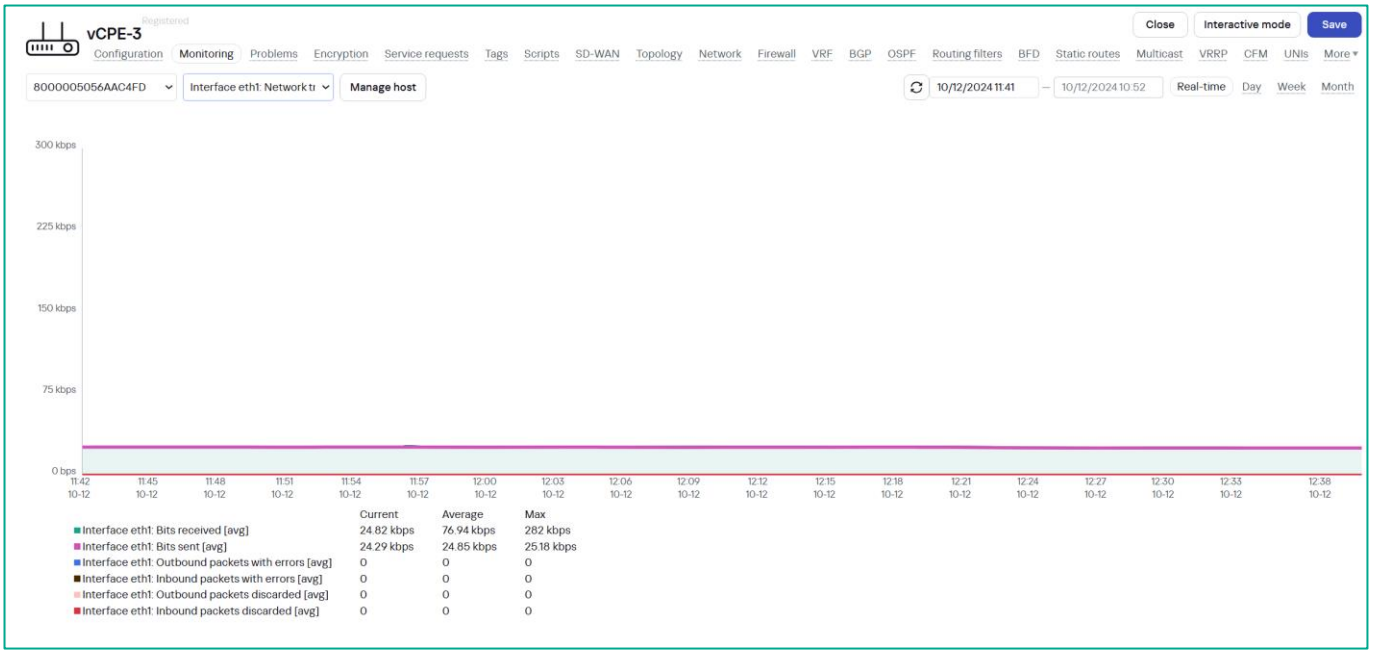
```
iperf3 -u -t 6000 -c <wst3 IP>
```



3.2.3. Проверить статистику трафика на WAN интерфейсах vCPE-3 в системе мониторинга.

Перейти в меню **CPE**, 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 в том, что через данный интерфейс не проходит тестовый сетевой трафик.



3.2.4. Проверка работы резервирования WAN интерфейсов.

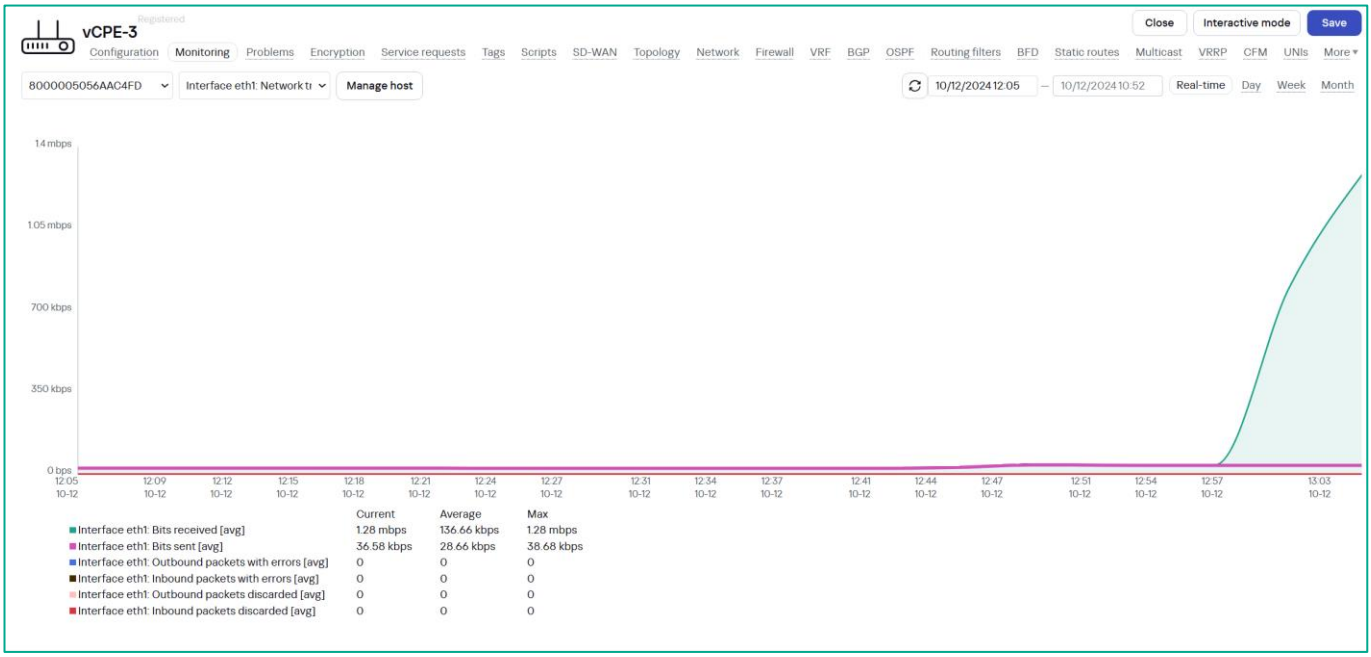
Сэмулировать отказ основного WAN-интерфейса:

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

```
ifconfig ens161 down
```

Из-за особенности работы iperf возможно потребуется перезапустить **iperf3** клиент на **wst-3**: повторить п. 3.2.2.

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



3.2.5. Вернуть настройки после завершения теста.

Включить сетевой интерфейс на хосте **isp**, отключенный в п. 3.1.5:

```
ifconfig ens161 up
```

Вернуть значения стоимости линков, измененное в п. 3.2.1, на значения по умолчанию.
Остановить процессы **iperf** на **wst3** и **wst4**, запущенные в п. 3.2.2 (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 линки для исключения потерь.

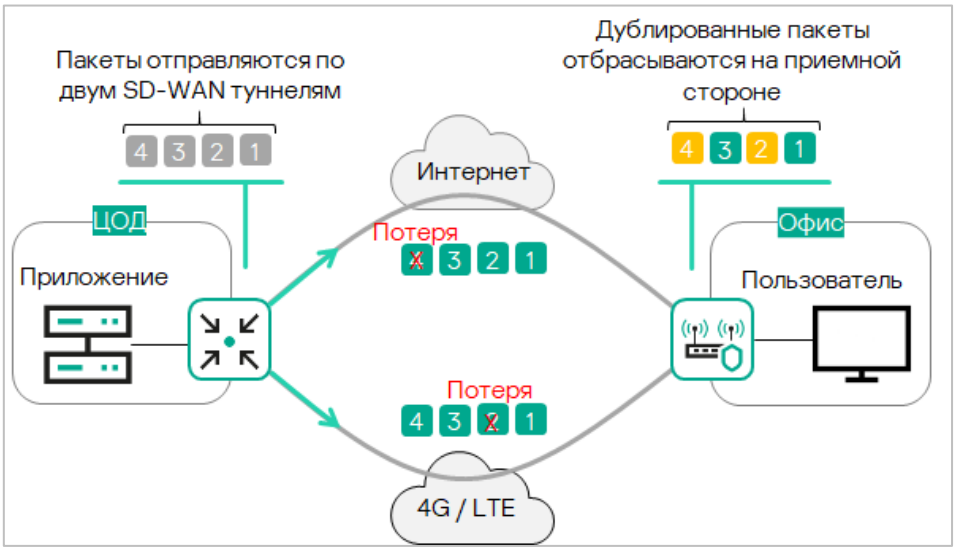


Рисунок 3.3.1 Дублирование пакетов

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

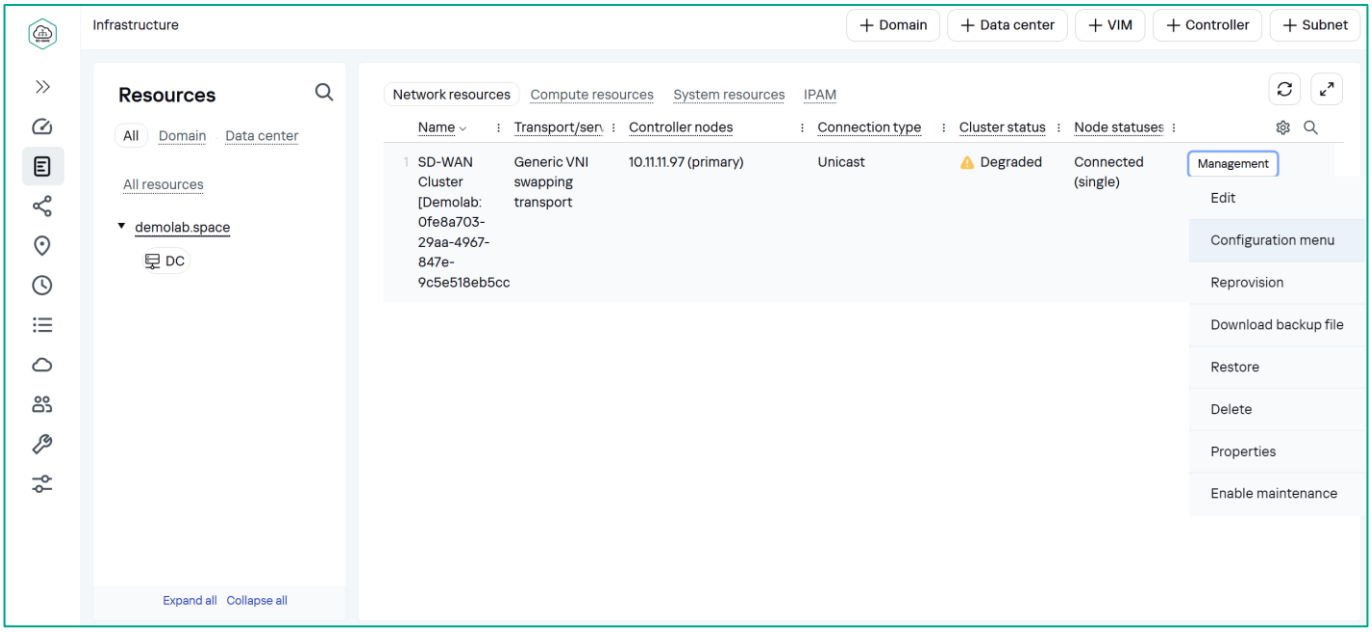
Для демонстрации резервирования трафика между vCPE-3 и srv1 на хостах wst3 и srv1 используется ICMP ping. Для проверки работы механизма дублирования будет использоваться tcpdump на vCPE-3.

3.3.1. Выбрать режим балансировки broadcast для транспортного сервиса.

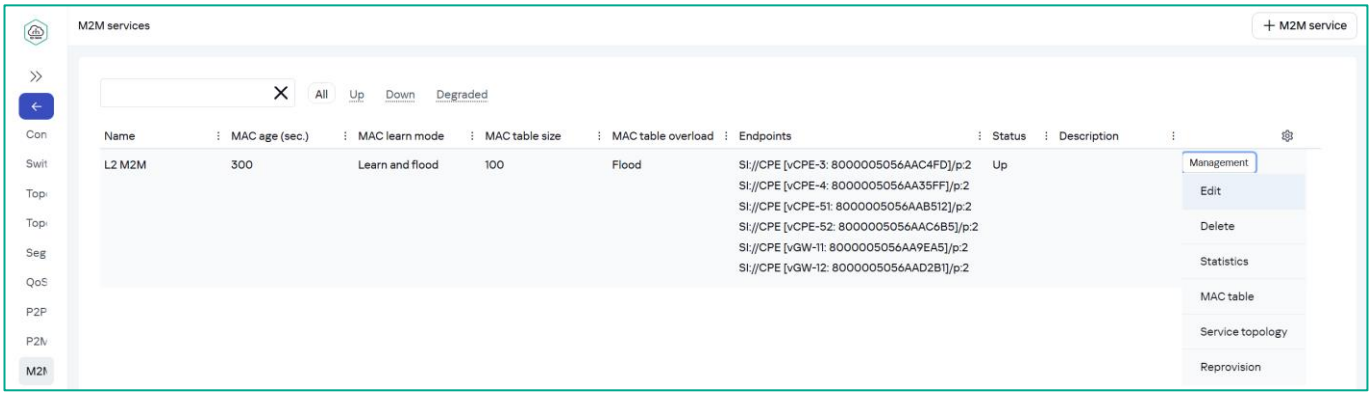
Доступные режимы балансировки:

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

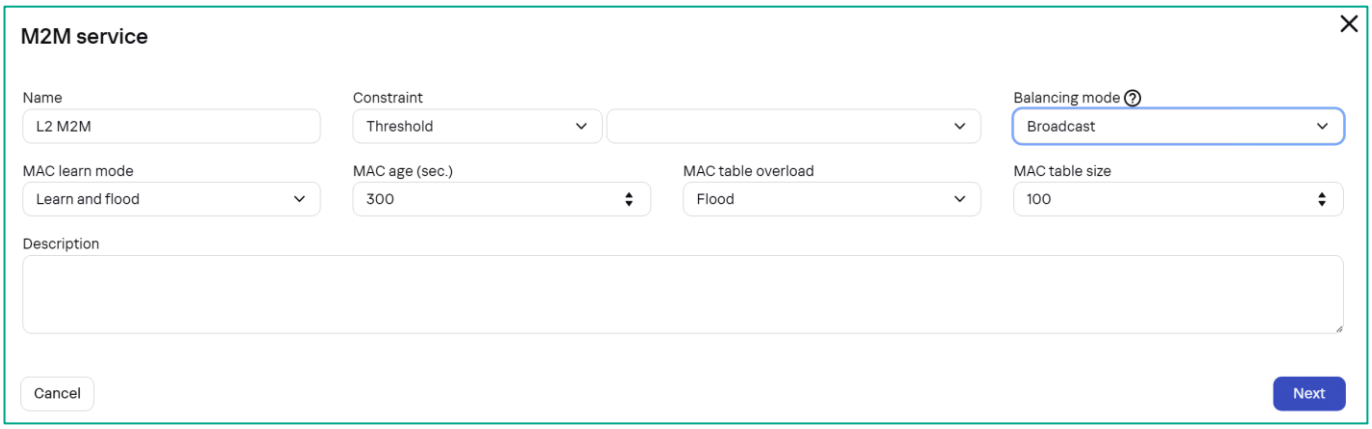
Для выбора режима балансировки перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu**



Перейти в меню **M2M services**. Выбрать транспортный сервис **L2 M2M** и нажать **Management → Edit**



Задать **Balancing mode**: **Broadcast**



Затем сохранить настройки сервиса: нажать **Next**, **Next** и **Save**

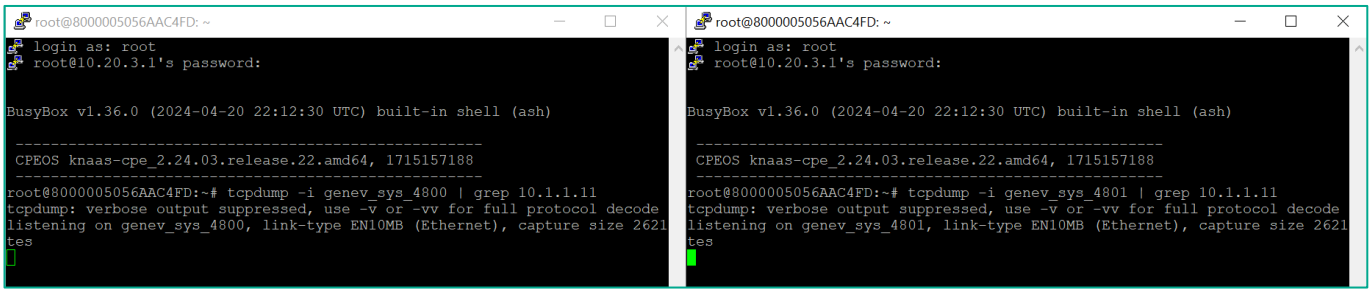
3.3.2. Проверить работу режима балансировки broadcast у транспортного сервиса.

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**:

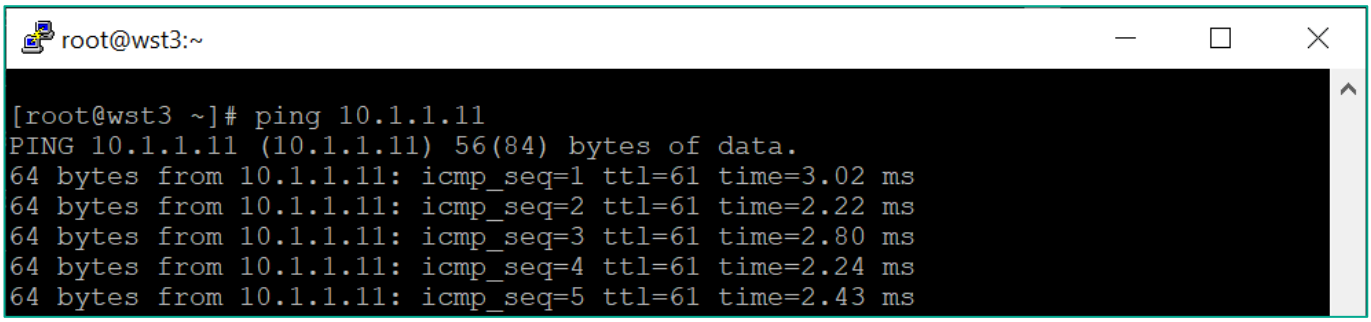
```
tcpdump -i genev_sys_4800 | grep 10.1.1.11

tcpdump -i genev_sys_4801 | grep 10.1.1.11
```

- **10.1.1.11** – адрес хоста **srv1**.
- **genev_sys** – туннельные интерфейсы CPE. Номер порта указывает на номер WAN интерфейса CPE 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).

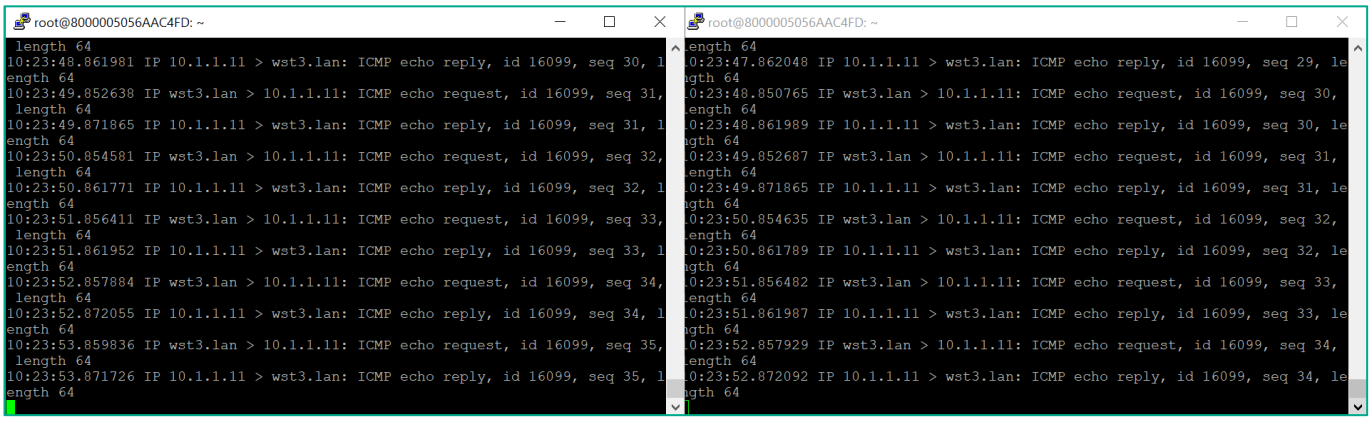


Запустить ICMP ping с **wst3** до **srv1**:

```
ping 10.1.1.11
```



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



3.3.3. Вернуть настройки после завершения теста.

Повторить п. 3.3.1 и изменить режим балансировки на **per-flow**.

Остановить ICMP **ping** на **wst3** и **tcpdump** на **vCPE-3**, запущенные в пункте 3.3.2 (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 CPE при наличии потерь на каналах передачи данных. Восстановление данных обеспечивается избыточным кодированием потока данных на устройстве, находящемся на передающей стороне.

Передающее устройство CPE кодирует поток выходящих через линк пакетов трафика с добавлением избыточных пакетов. Степень избыточности можно настроить через параметры контроллера SD-WAN или на отдельном линке.

Принимающее устройство CPE буферизует принятые через линки 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 линках) для уменьшения коэффициента потери пакетов трафика и увеличения скорости TCP-соединений.

Для получения дополнительной информации обратитесь к Kaspersky SD-WAN Online Help: https://support.kaspersky.com/help/SD-WAN/2.3/ru-RU/245033.htm

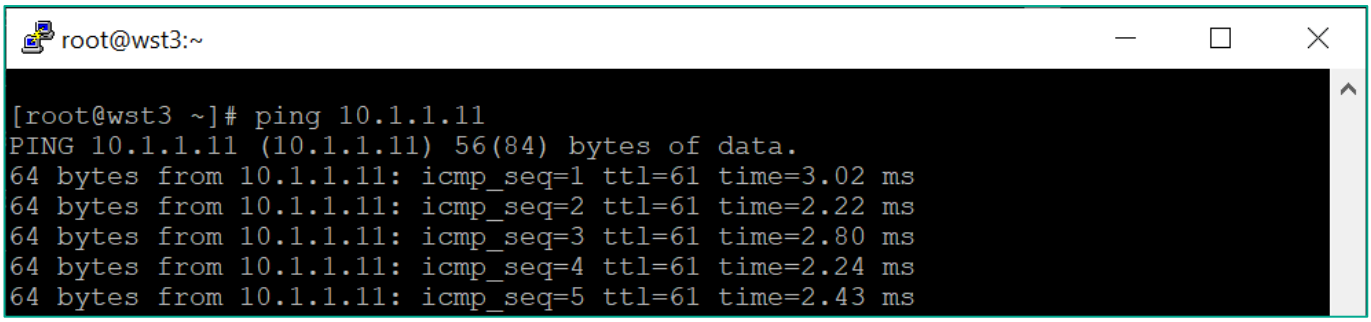
В данном сценарии рассматривается сценарий с эмуляцией потерь на канале, измерением качества линков и включением FEC для восстановления потерянных пакетов. Тестовый трафик будет генерироваться между рабочими станциями wst3 и srv1 с использованием ICMP ping.

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

3.4.1. Сгенерировать тестовый трафик между wst3 и srv1.

Запустить icmp **ping** с хоста **wst3** до **srv1**:

```
ping 10.1.1.11
```



3.4.2. Сэмулировать потери пакетов на хосте isp с помощью TC.

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

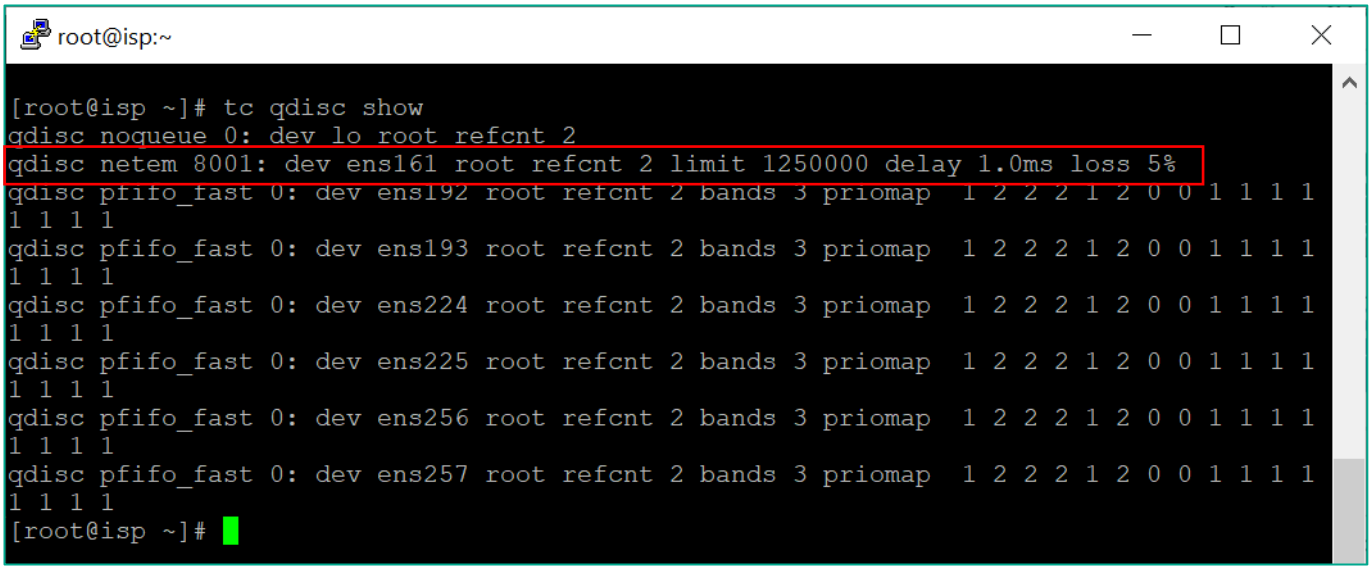
Подключиться к хосту **isp** и выполнить команду:

```
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 **1 ms** с разбросом в **0 ms**, **limit** – выделяет буфер в **1250000** байт для обработки данных TC.

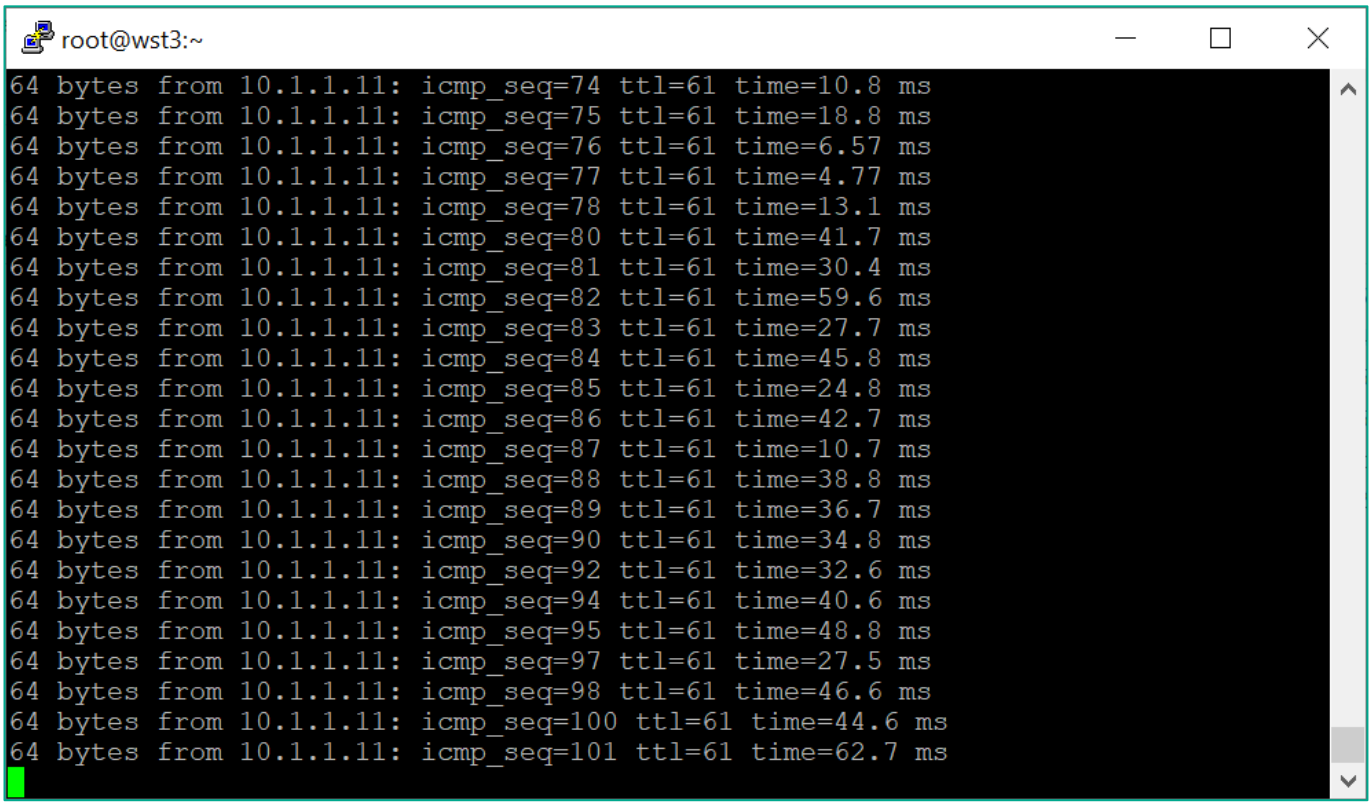
Проверить примененные настройки с помощью следующей команды:

```
tc qdisc show
```



Note: По умолчанию режим балансировки per-flow, поэтому поток может пойти через другой интерфейс, и эмуляция потерь не применится на интерфейс, через который будет проходить поток трафика. В данном сценарии используется режим per-flow.

Как видно ниже по **ICMP sequence number**, присутствуют потери пакетов: видны пропущенные ответы (пропущены **sequence 79**, **91**, **96**, **99**).



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 (в сторону **eth1** на **vCPE-3**):

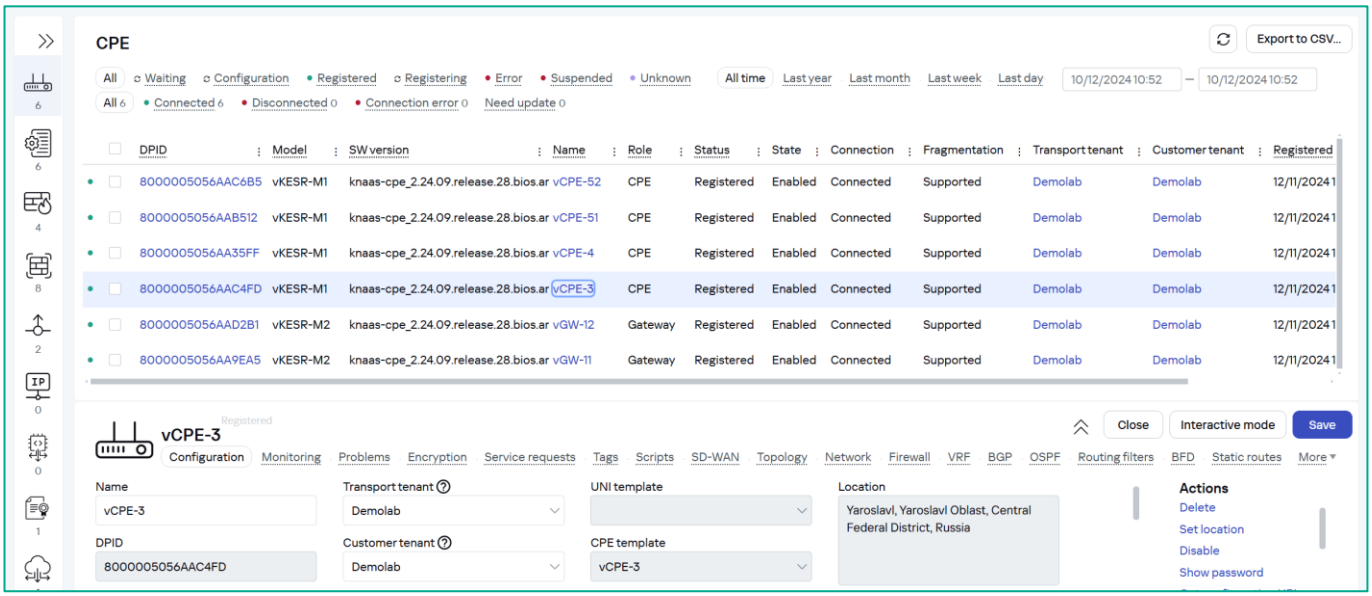
```
tc qdisc add dev ens193 root netem delay 1ms 0ms limit 1250000 loss 5%
```

Затем снять задержку с первого сетевого интерфейса (в сторону **eth0** на **vCPE-3**):

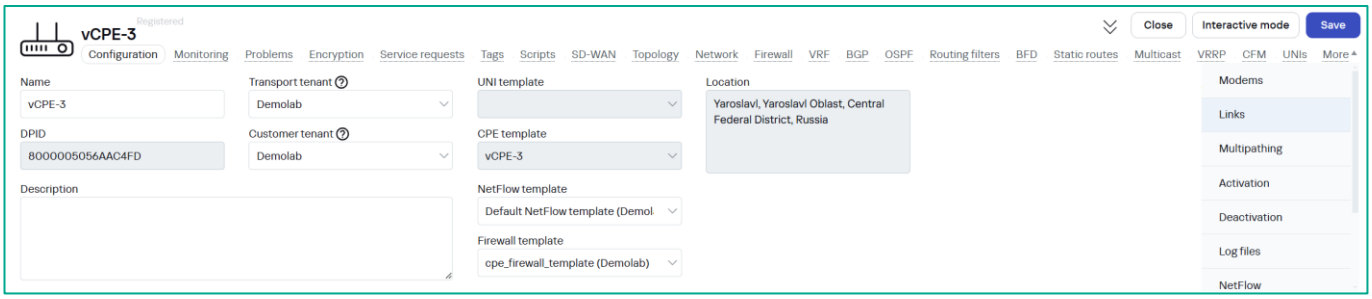
```
tc qdisc del dev ens161 root
```

3.4.3. Включить мониторинг потерь пакетов на линках vCPE-3.

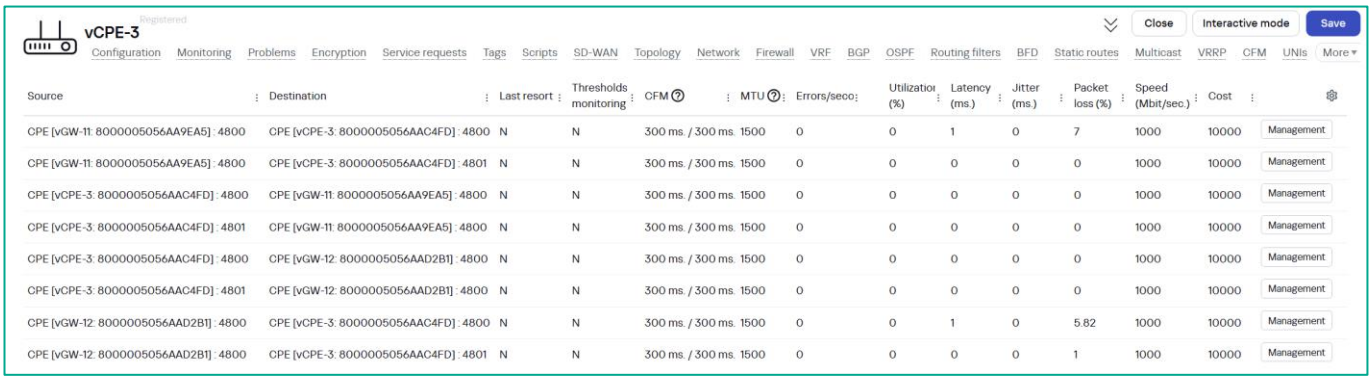
Перейти в меню **CPE** и выбрать **vCPE-3**.



Перейти на вкладку **Links**.



Отобразится список построенных линков с **vCPE-3**.

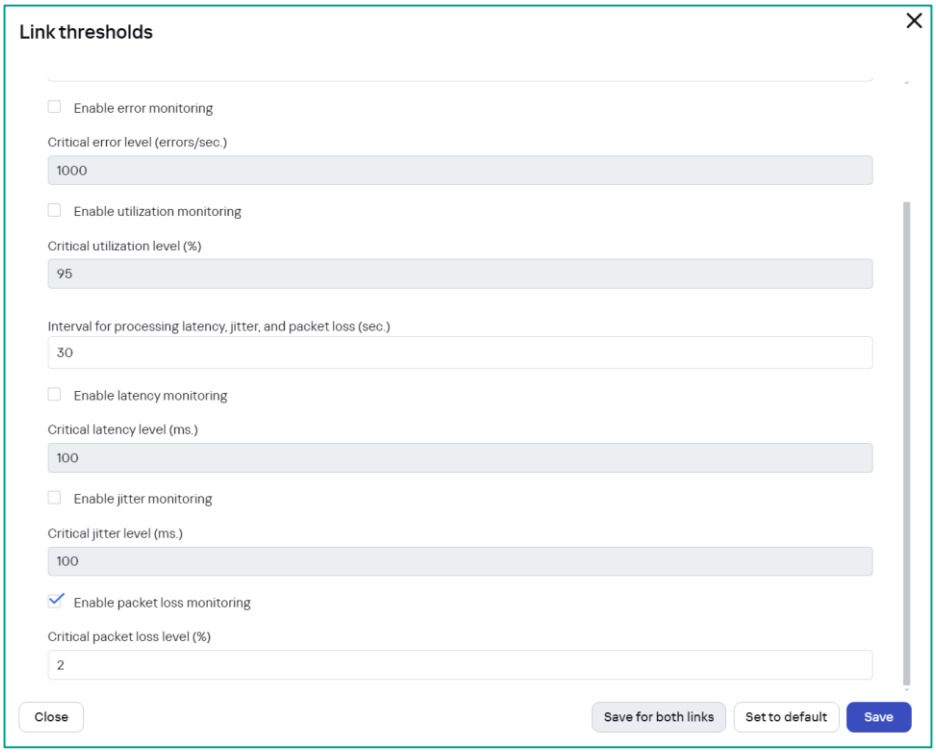


Для всех линков поочередно нажать **Management → Set thresholds**

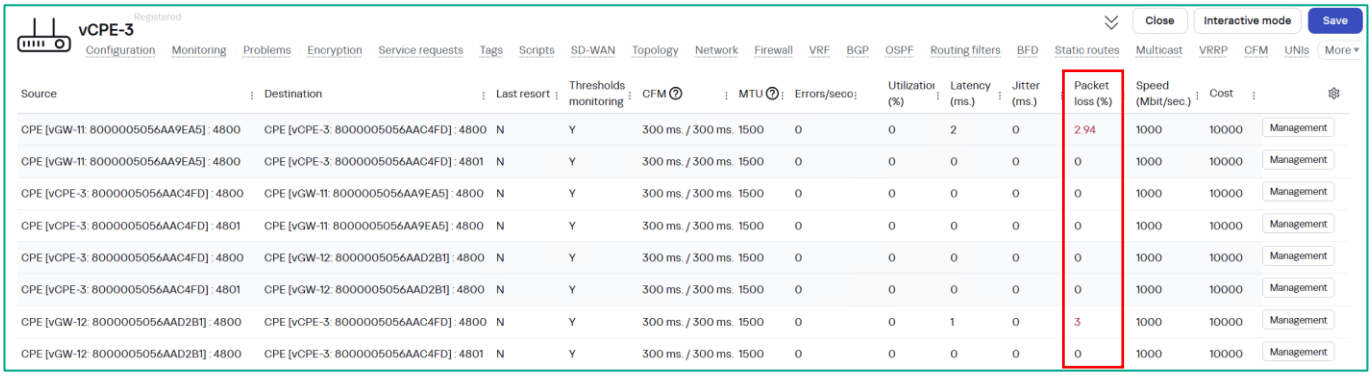
Задать параметры мониторинга линков:

- Отметить **Enable tunnel thresholds monitoring**
- **Enable packet loss monitoring → Critical packet loss level: 2%**

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

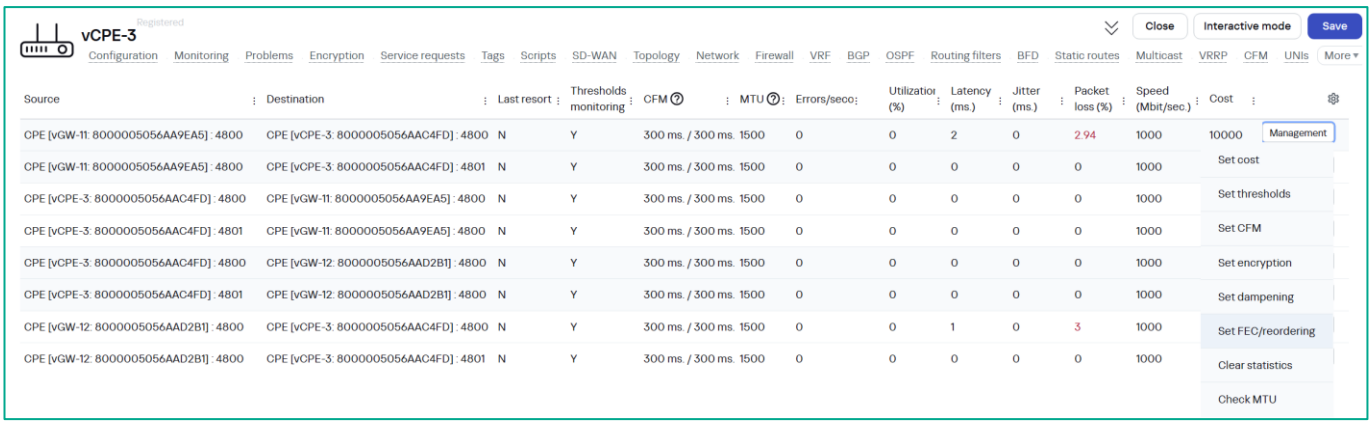


После применения настроек отобразится статистика потерь на линках. Значения измеренных параметров, не удовлетворяющих порогам, заданных ранее, будут выделены красным цветом. Т.к. задержка эмулировалась в сторону интерфейса **sdwan0(eth0) vCPE-3**, то **packet loss** наблюдается на соответствующих линках от **vGW-11** и **vGW-12**, проходящих через данный интерфейс.



3.4.4. Включить FEC для линков vCPE-3, на которых наблюдаются потери.

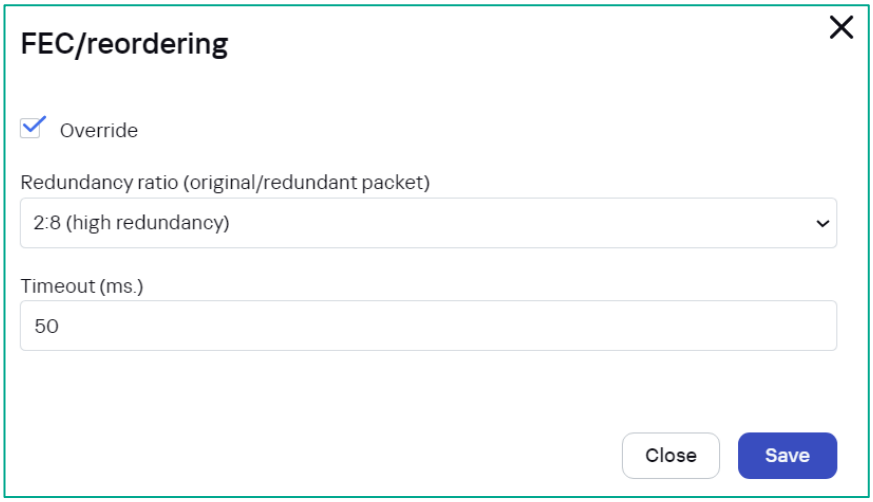
Поочередно для каждого линка, на котором наблюдается критический уровень потерь, выбрать **Management → Set FEC/reordering**



Задать параметры FEC для линков:

- Отметить **Override**
- **Redundancy ratio**: **2:8**
- **Timeout**: **50**

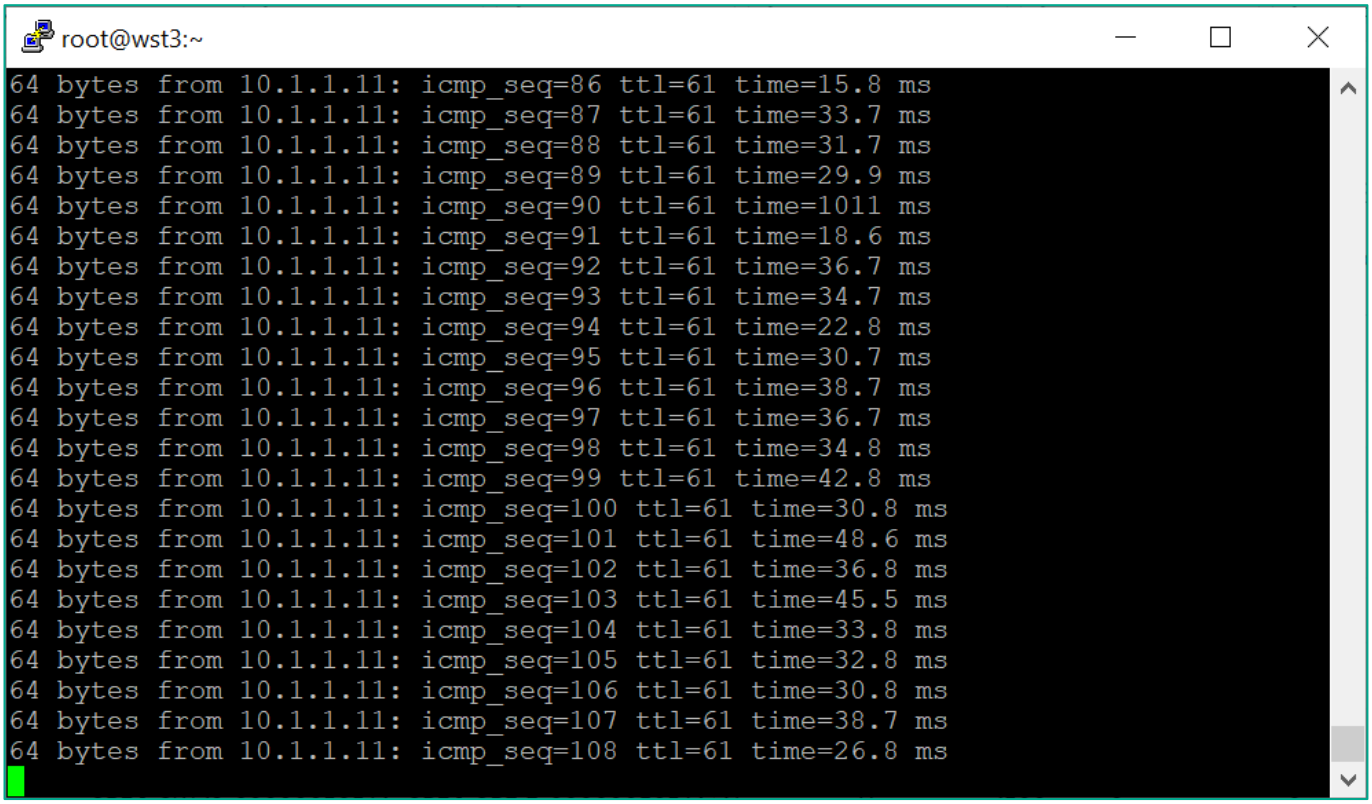
Нажать **Save**



3.4.5. Проверить работу FEC в статистике ping wst3.

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.



3.4.6. Вернуть настройки после завершения теста.

Повторить п. 3.4.3 и выключить мониторинг потерь пакетов для линков.

Выполнить п. 3.4.4 и выключить FEC на линках.

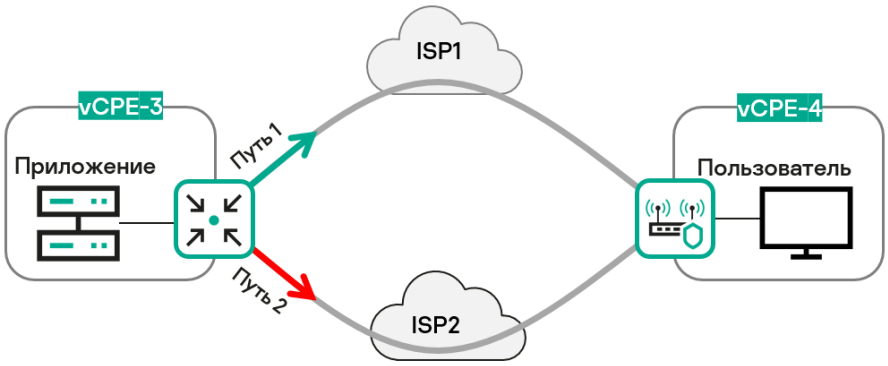
Остановить ICMP ping на **wst3**, запущенный в пункте 3.4.1 (возможно прервать с помощью `Ctrl+Z`).

Выключить эмуляцию задержек и джиттера на хосте **isp**:

```
tc qdisc del dev ens161 root netem

tc qdisc del dev ens193 root netem
```

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

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



	Джиттер	Потери пакетов	Задержка
Путь 1	71 ms	0 %	297
Путь 2	4 ms	2 %	15

Рис. 3.5.1 Мониторинг качества линков

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

https://support.kaspersky.com/help/SD-WAN/2.3/ru-RU/244988.htm

Ниже рассматривается сценарий с измерением задержки и джиттера на линках, заданием ограничений и перенаправление трафика на линки, 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 Linux Traffic Control.

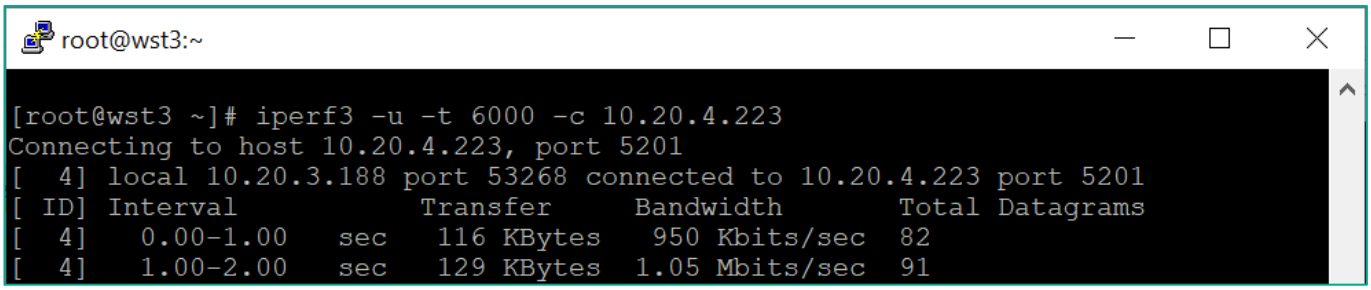
Будут созданы ограничения для транспортного сервиса с целью исключения линков, не удовлетворяющих заданным параметрам джиттера и задержек.

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

3.5.1. Сгенерировать тестовый трафик между wst3 и srv1.

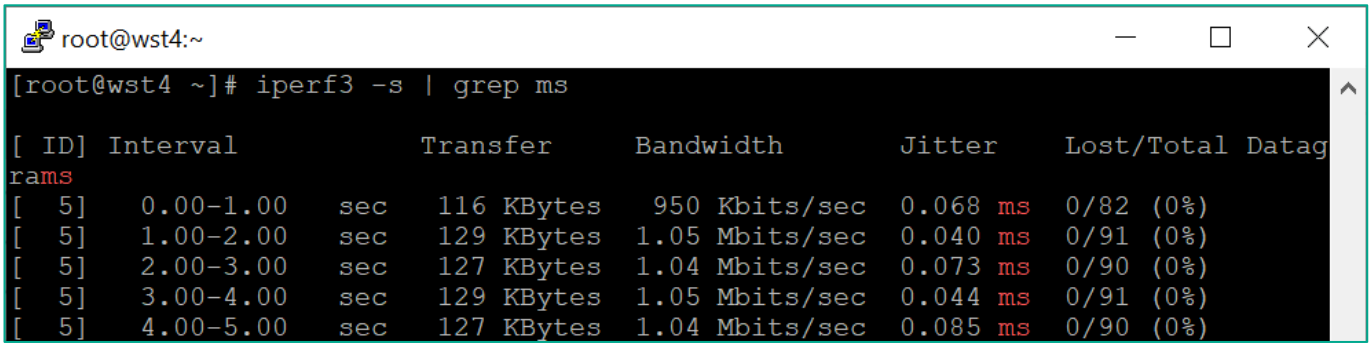
Запустить сервер **iperf** на хосте **wst4**:

```
iperf3 -s | grep ms
```



Запустить клиент **iperf** на хосте **wst3**:

```
iperf3 -u -t 6000 -c <wst4 IP address>
```



3.5.2. Сэмулировать задержку и джиттер на интерфейсе в сторону vCPE-3 с помощью TC.

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

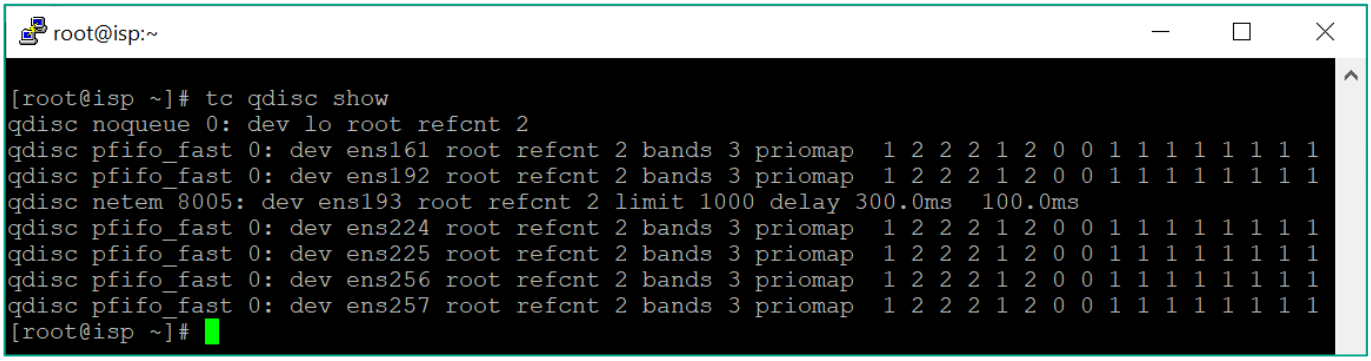
Подключиться к хосту **isp** и выполнить команду:

```
tc qdisc add dev ens193 root netem delay 300ms 100ms
```

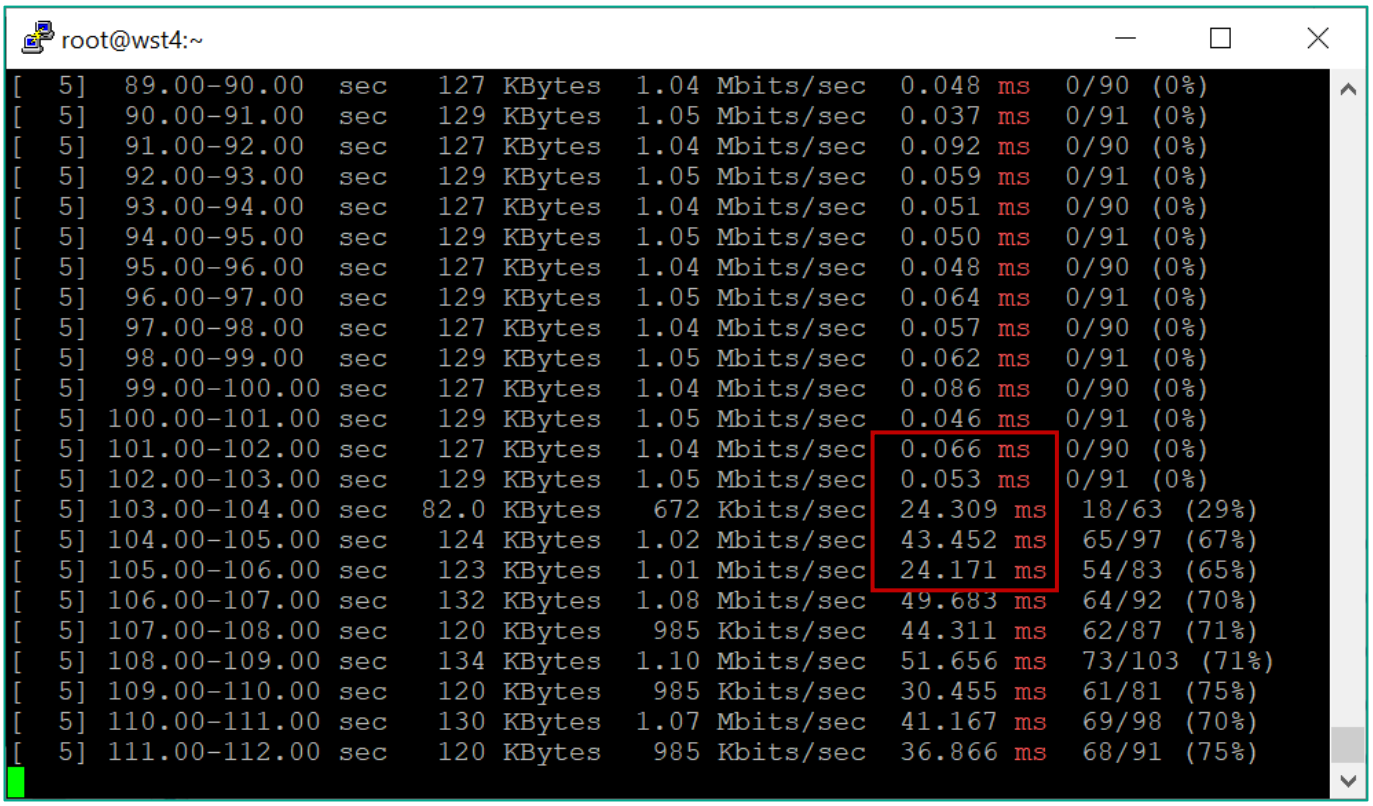
Данная команда создает задержку (**delay**) в **300ms** с разбросом (**jitter**) в **100ms**.

Проверить примененные настройки с помощью следующей команды:

```
tc qdisc show
```



Проверить наличие джиттера в статистике **iperf** на рабочей станции **wst4**.



Note: по умолчанию режим балансировки per-flow, поэтому поток может пойти через другой интерфейс, и джиттера может не быть видно в статистике iperf.

Если в статистике не будет видно задержку, то необходимо на хосте **isp** применить эмуляцию на другой интерфейс (в сторону интерфейса **eth0** на **vCPE-3**):

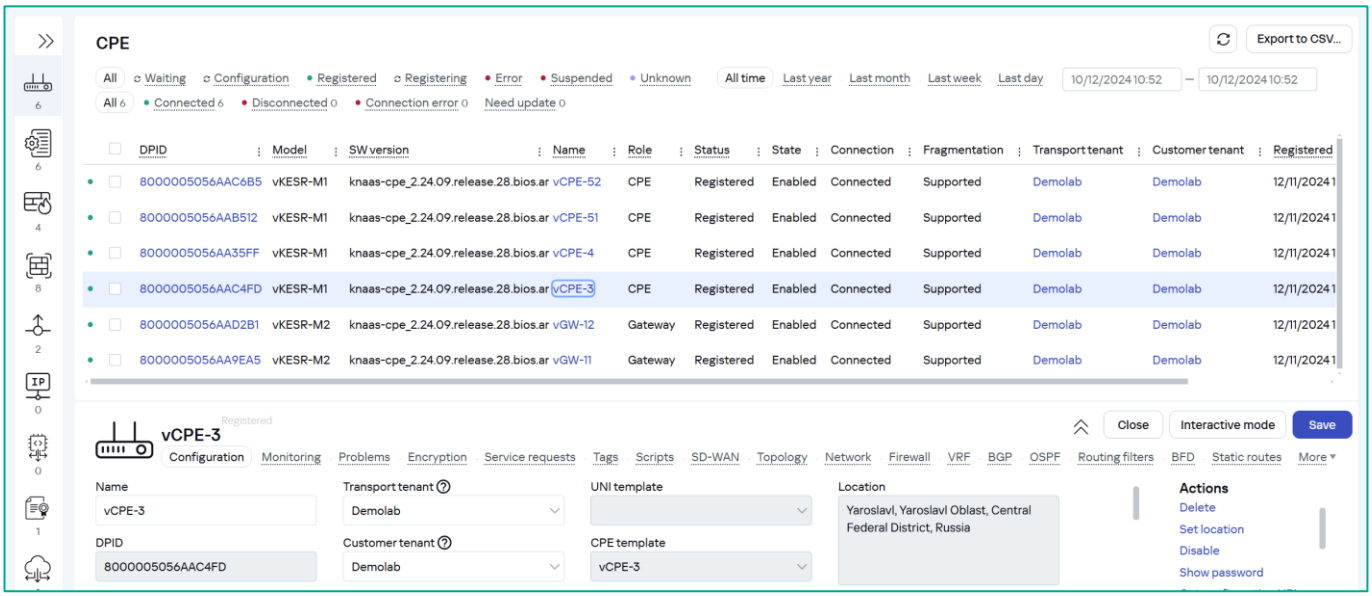
```
tc qdisc add dev ens161 root netem delay 300ms 100ms
```

Затем снять задержку с первого сетевого интерфейса (в сторону интерфейса **eth1** на **vCPE-3**):

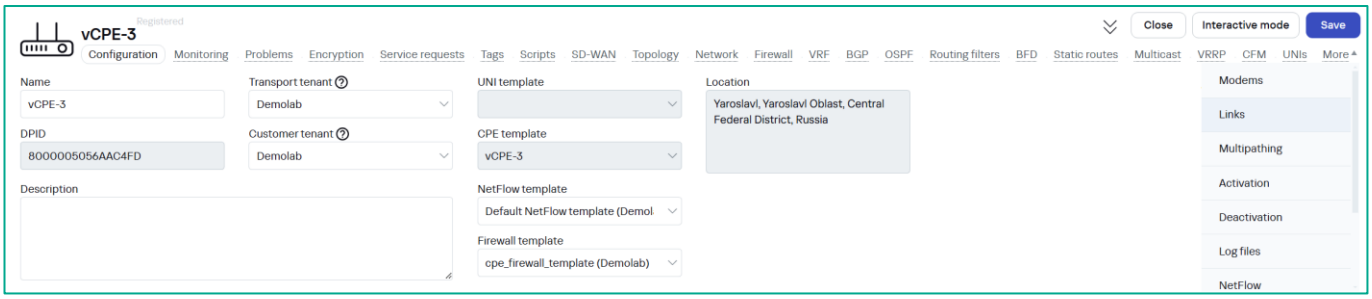
```
tc qdisc del dev ens193 root
```

3.5.3. Включить мониторинг задержек и джиттера на линках vCPE-3.

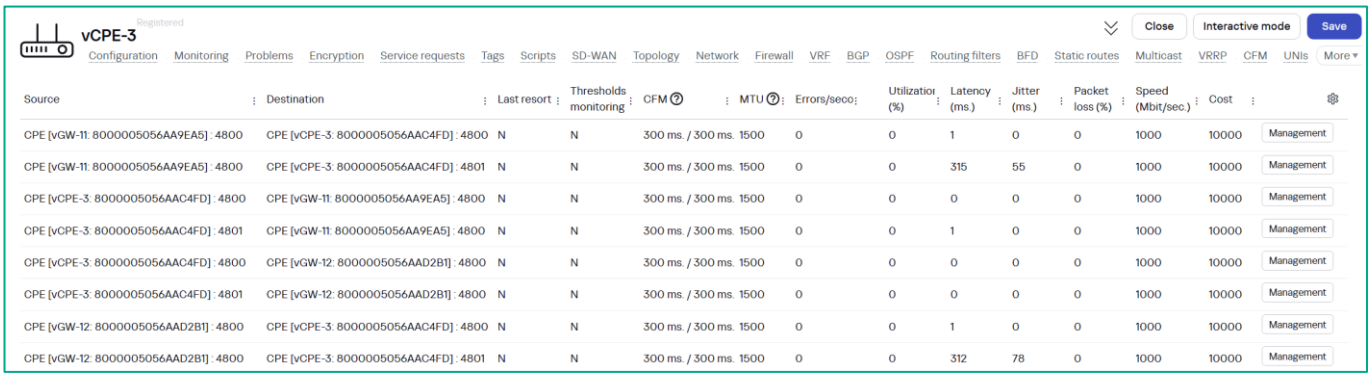
Перейти в меню **CPE** и выбрать **vCPE-3**.



Перейти на вкладку **Links**.



Отобразится список построенных линков с **vCPE-3**.

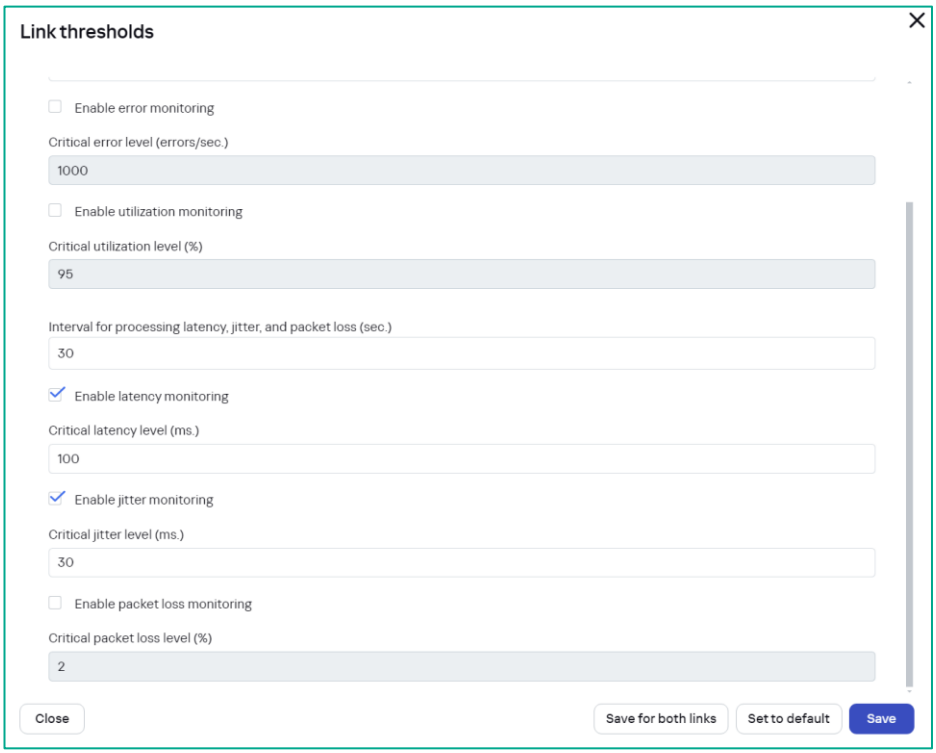


Для всех линков поочередно нажать **Management → Set thresholds**

Задать параметры мониторинга линков:

- Отметить **Enable tunnel thresholds monitoring**
- **Enable latency monitoring → Critical latency level**: **100 msec**
- **Enable jittter monitoring → Critical jitter level**: **30 msec**

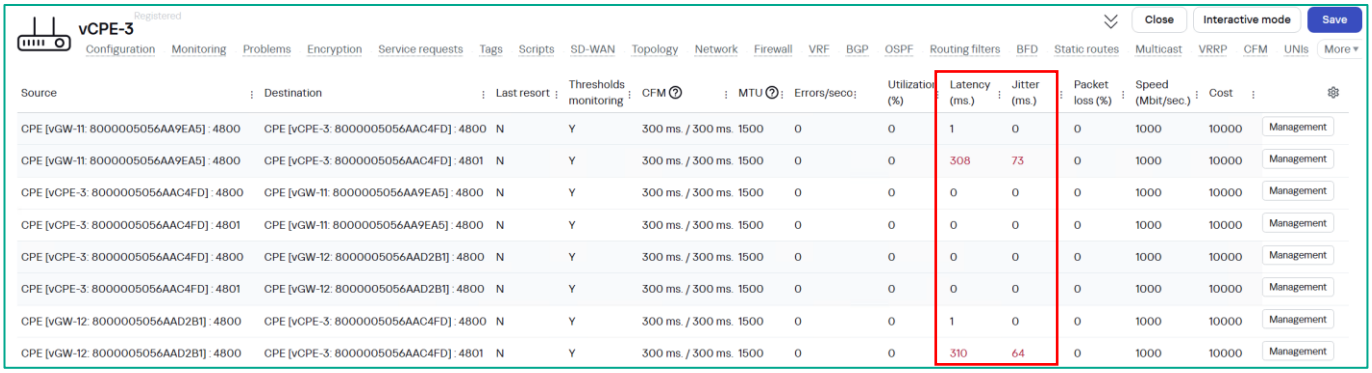
Нажать **Save for both links** – сохранение параметров мониторинга линков в оба направления.



Данные настройки включат мониторинг задержек и джиттера для линков и зададут пороговые значения в 100мс и 30мс соответственно.

Повторить эти действия для всех линков **vCPE-3**.

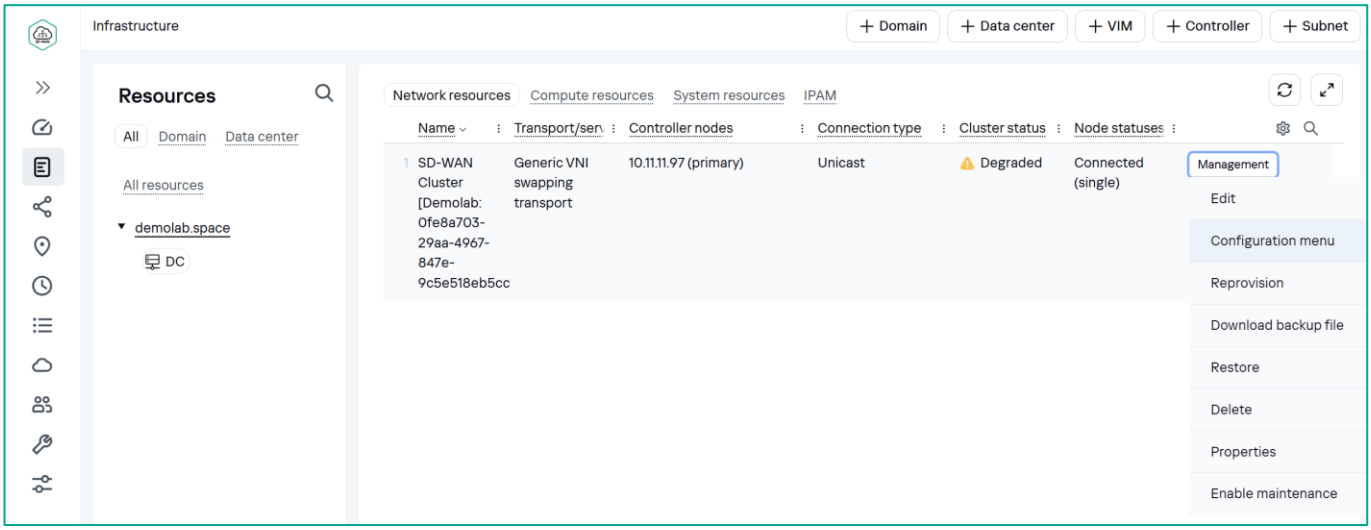
После применения настроек мониторинга линков отобразится статистика задержек и джиттера. Значения параметров, не удовлетворяющих заданным порогам, будут выделены красным цветом.



3.5.4. Создать пороговое ограничение для исключения линков, не удовлетворяющих заданным порогам по задержке и джиттеру.

Для перенаправления трафика необходимо создать пороговые ограничения (**Constraints**).

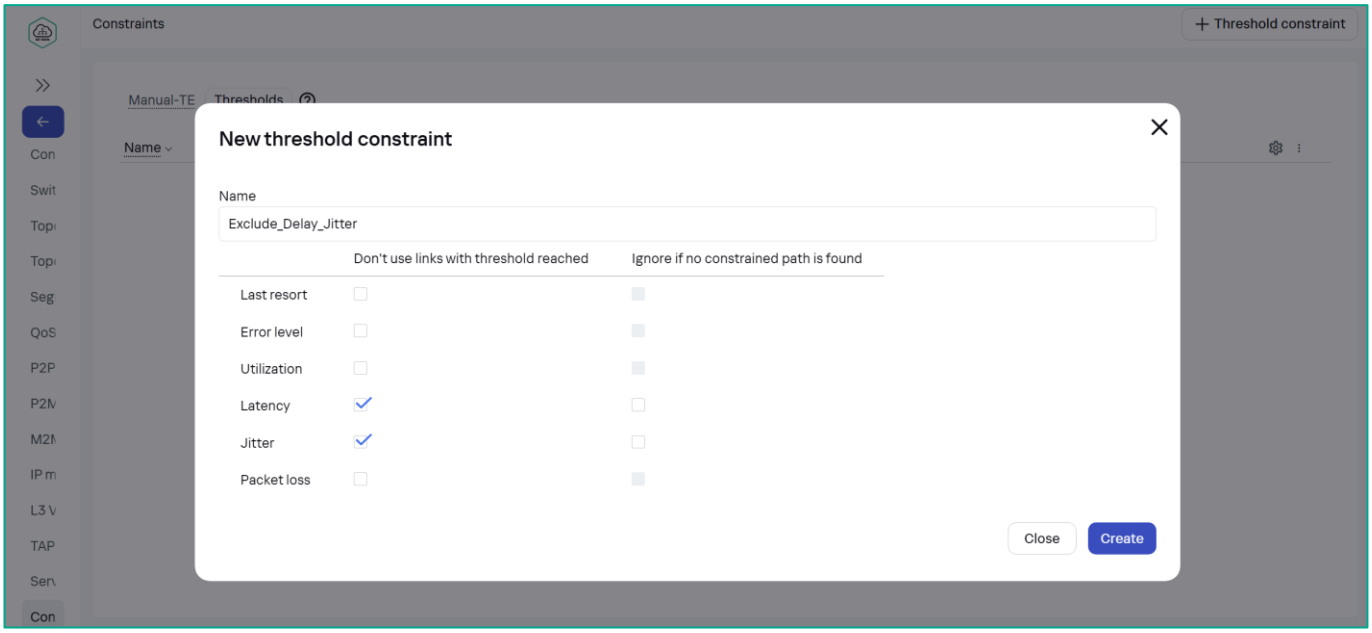
Перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu**



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

Задать параметры порогового ограничения:

- Название (в примере **Exclude_Delay_Jitter**)
- Отметить **Latency** (ограничение для задержки)
- Отметить **Jitter** (ограничение для джиттера)



Нажать **Create**

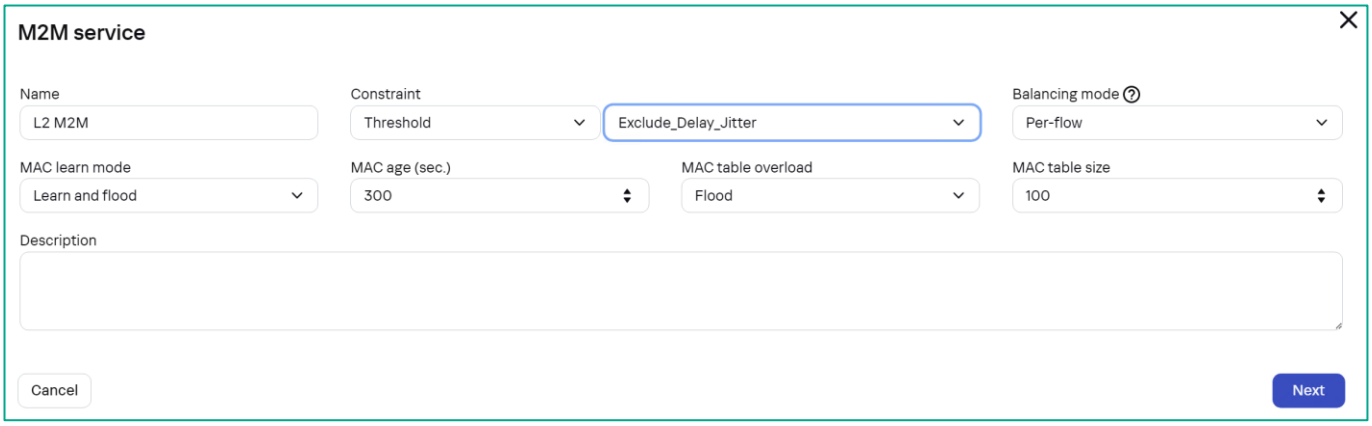
Данное пороговое ограничение исключит из путей прохождения трафика линки, не отвечающие настроенным в п. 3.5.3 пороговым значениям.

3.5.5. Применить созданное ограничение к транспортному сервису.

Перейти на вкладку **M2M Services**.

Открыть сервис **L2 M2M** для редактирования: **Management → Edit**

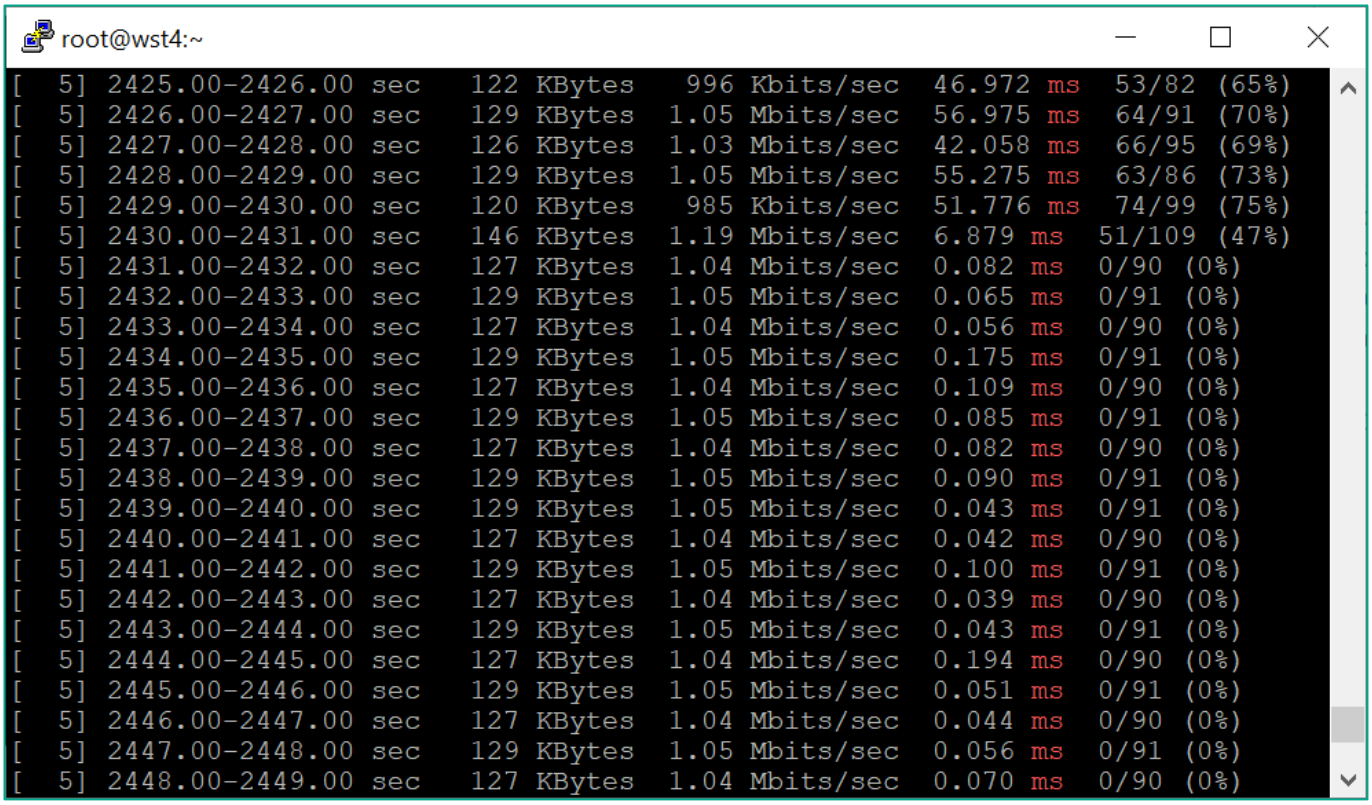
Выбрать созданное в п. 3.5.4 пороговое ограничение в секции **Constraint**



Нажать **Next, Next** и **Save** для сохранения изменений сервиса

После применения порогового ограничения контроллер SD-WAN уберет трафик с линков, не удовлетворяющих пороговым значениям.

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



3.5.6. Вернуть настройки после завершения теста.

Снять ограничение с транспортного сервиса: повторить п. 3.5.5 и убрать **constraint** (пороговое ограничение) из транспортного сервиса.

Выключить эмуляцию задержек и джиттера на хосте **isp**:

```
tc qdisc del dev ens161 root

tc qdisc del dev ens193 root
```

Выключить мониторинг задержек и джиттера на линках **vCPE-3**: повторить п. 3.4.3.

Остановить **iperf** на **wst3** и **wst4**, запущенный в пункте 3.5.3 (возможно прервать с помощью `Ctrl+Z`).

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 линки с задержкой, не удовлетворяющей заданным пороговым значениям.

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

https://support.kaspersky.com/help/SD-WAN/2.3/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 сервисный интерфейс типа ACL для перенаправления трафика в отдельный сервис.

Линки, проходящие через интерфейс sdwan0 (eth0) vCPE-3 будут отмечены как “Last resort” («нежелательные» для использования). Будет создан отдельный транспортный сервис для приоритетного трафика. Для данного сервиса будут заданы ограничения (Constraints), которые исключат линки, отмеченные как Last resort из пути прохождения трафика. Для проверки переключения трафика будет использоваться tcpdump на vCPE-3.

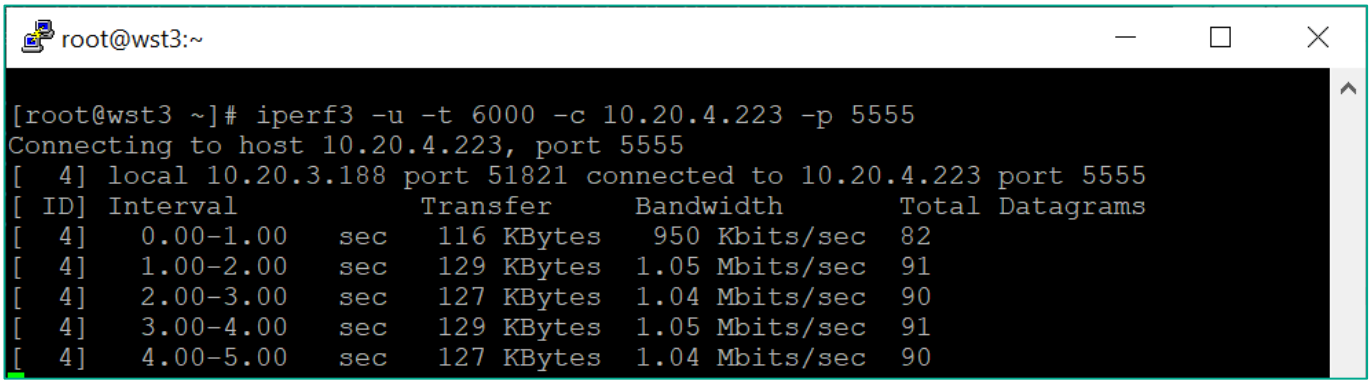
3.6.1. Сгенерировать тестовый трафик между wst3 и wst4.

Запустить сервер **iperf** на хосте **wst4** портом **5555**:

```
iperf3 -s -p 5555
```

Запустить клиент **iperf** на хосте **wst3** с портом **5555**:

```
iperf3 -u -t 6000 -c <wst4 IP address> -p 5555
```



3.6.2. Проверить, через какой туннельный интерфейс отправляется тестовый трафик.

Подключиться к **vCPE-3** по SSH и запустить **tcpdump** для отображения пакетов, проходящих через туннельный интерфейс **genev_sys_4800**:

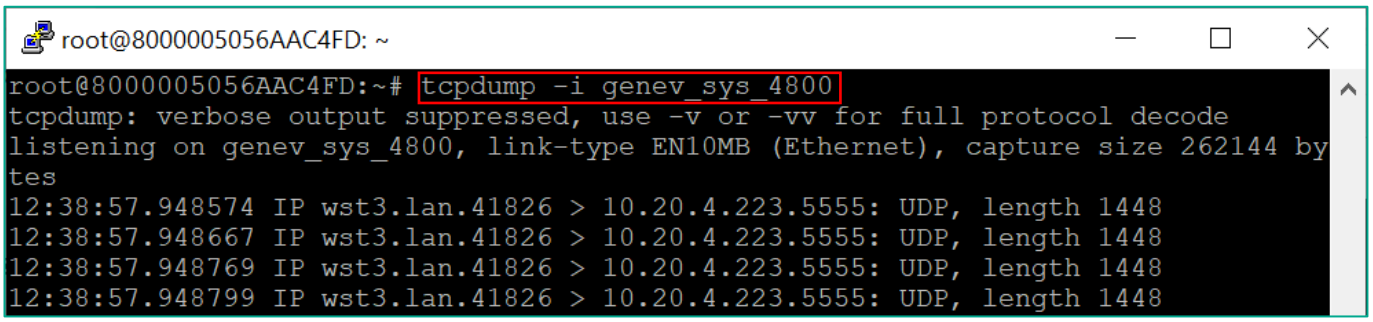
```
tcpdump -i genev_sys_4800
```

Если тестовый трафик проходит через туннельный интерфейс, то в выводе **tcpdump** будут видны UDP пакеты, отправленные iperf3 на порт **5555**.

Определить по выводу tcpdump через какой интерфейс проходит тестовый трафик: **genev_sys_4800** или **genev_sys_4801**.

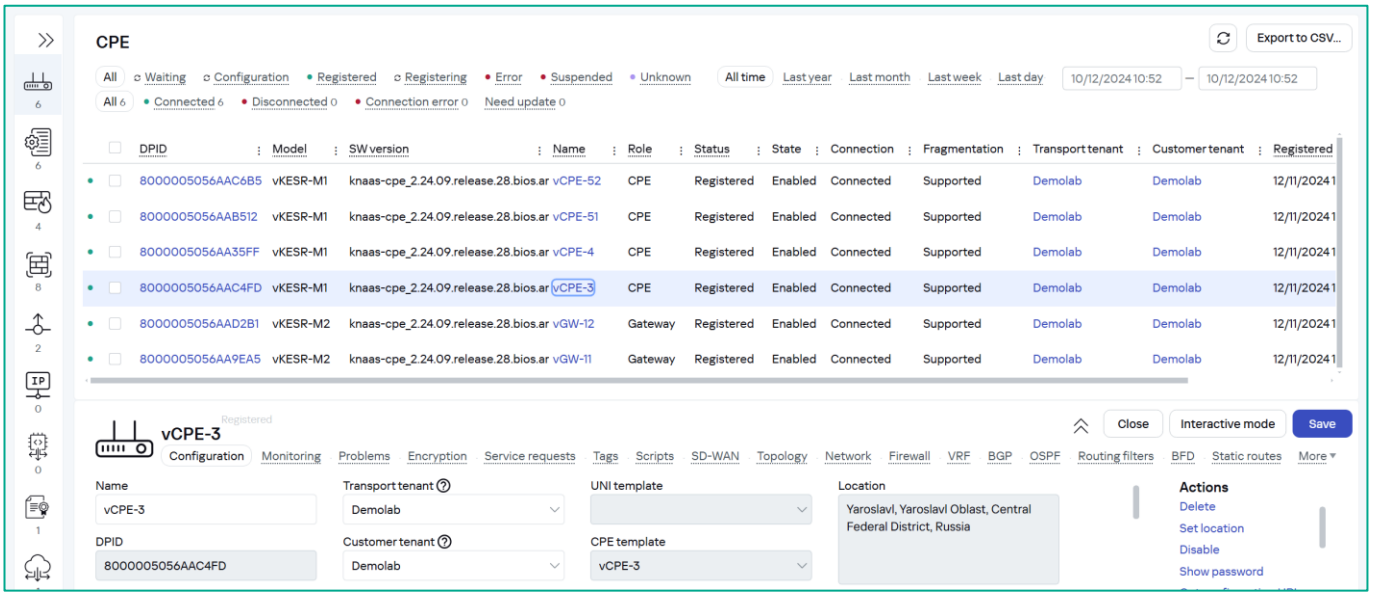
genev_sys – туннельные интерфейсы CPE. Номер порта указывает на номер WAN интерфейса CPE устройства. Номера назначаются по порядку, начиная с порта 4800, по одному на каждый WAN интерфейс. Порт **4800** означает WAN интерфейс **sdwan0** (eth0), порт **4801** означает WAN интерфейс **sdwan1** (eth1).

В данном примере трафик проходит через интерфейс **genev_sys_4800**.

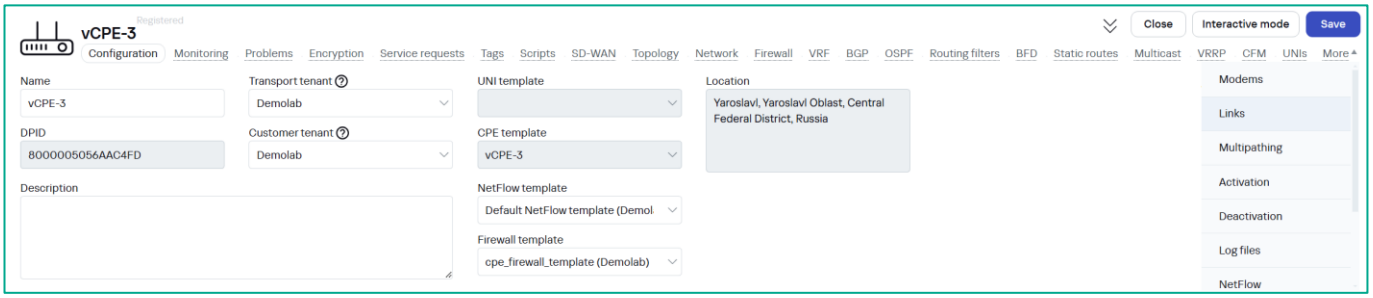


3.6.3. Задать параметр Last resort для линков vCPE-3.

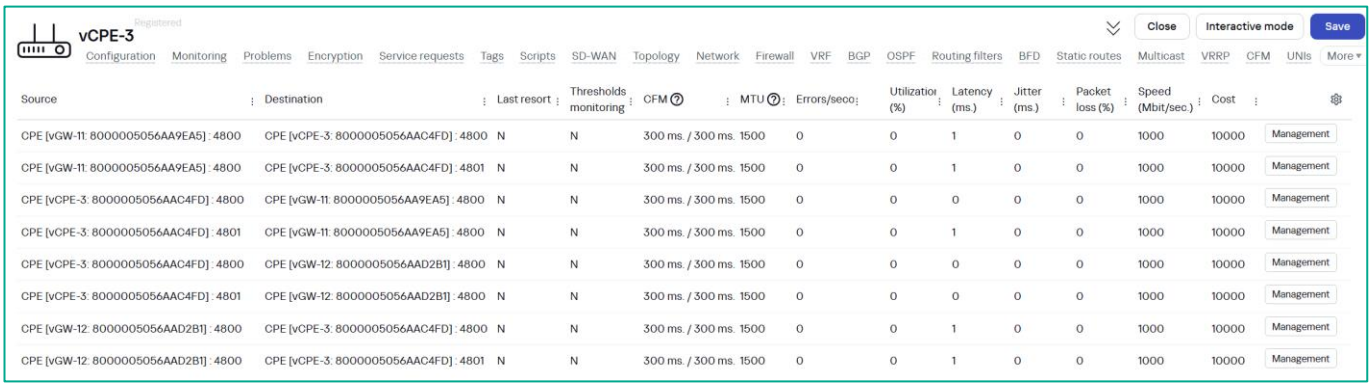
Перейти в меню **CPE** и выбрать **vCPE-3**.



Перейти на вкладку **Links**.



Отобразится список построенных линков с **vCPE-3**.



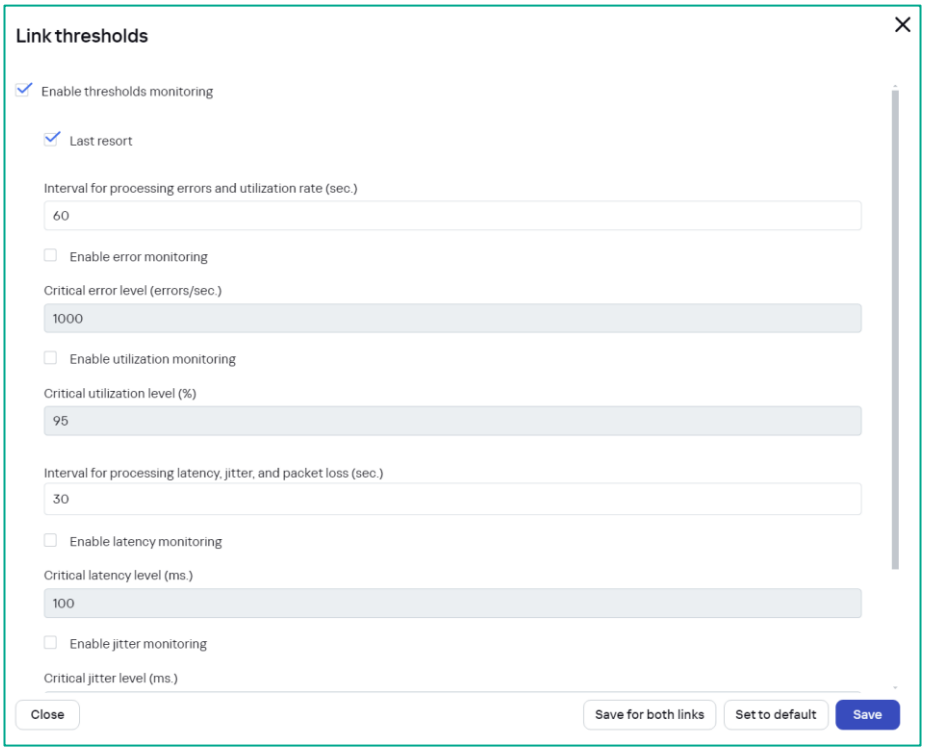
Найти все линки, через которые проходит трафик: порты источника или назначения линков (4800 или 4801) должны совпадать с номером туннельного интерфейса CPE согласно проверке в пункте 3.6.2. В данном примере трафик проходит через интерфейс **genev_sys_4800**

Линки, через которые проходит трафик в данном 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**

Для всех найденных линков поочередно нажать **Management → Set thresholds** и задать параметр **Last resort** для линков:

- Отметить **Enable tunnel thresholds monitoring**
- Отметить **Last resort**

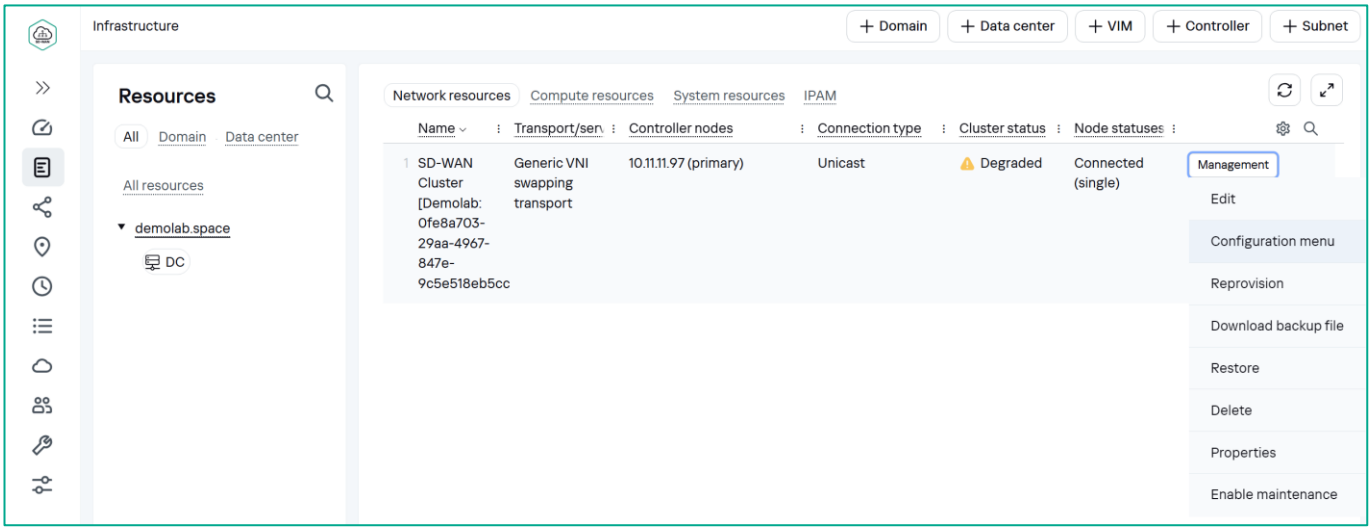


Нажать **Save for both links** – сохранение параметров мониторинга линков в оба направления.

3.6.4. Создать пороговое ограничение для исключения линков с параметром Last resort.

Для перенаправления трафика необходимо создать пороговые ограничения (**Constraints**).

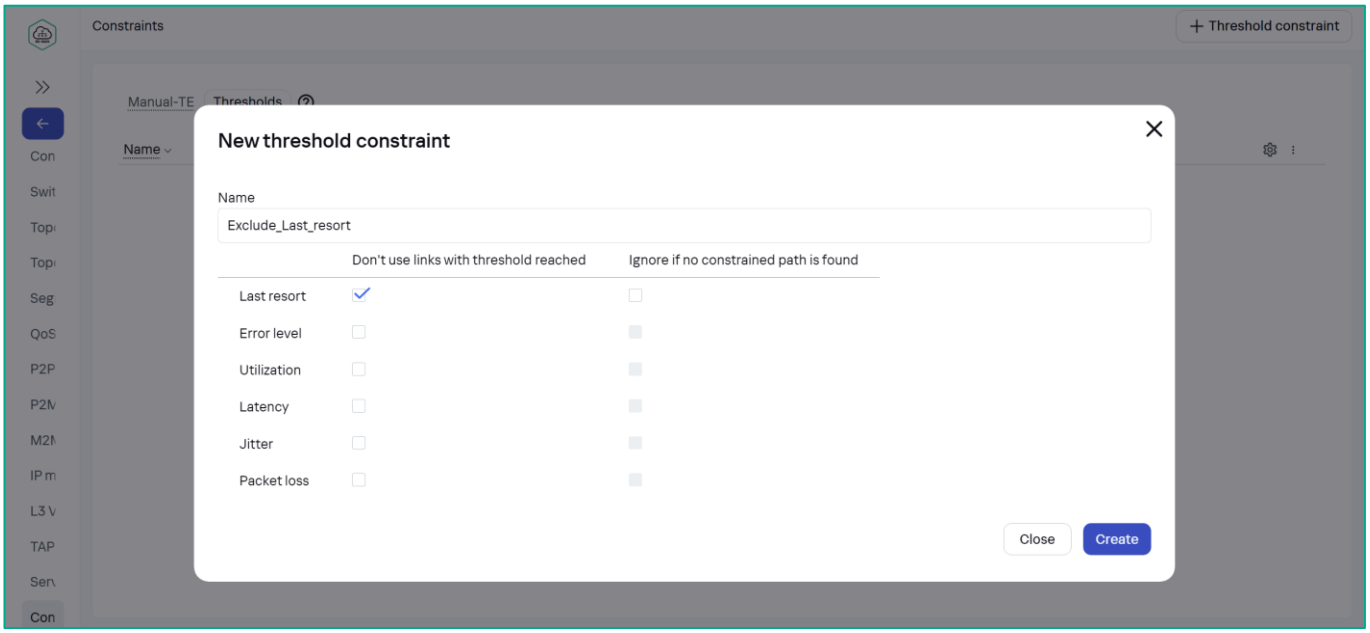
Перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu**



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

Задать параметры порогового ограничения:

- Название (в примере **Exclude_Last_resort**)
- Отметить ограничение для **Last resort**



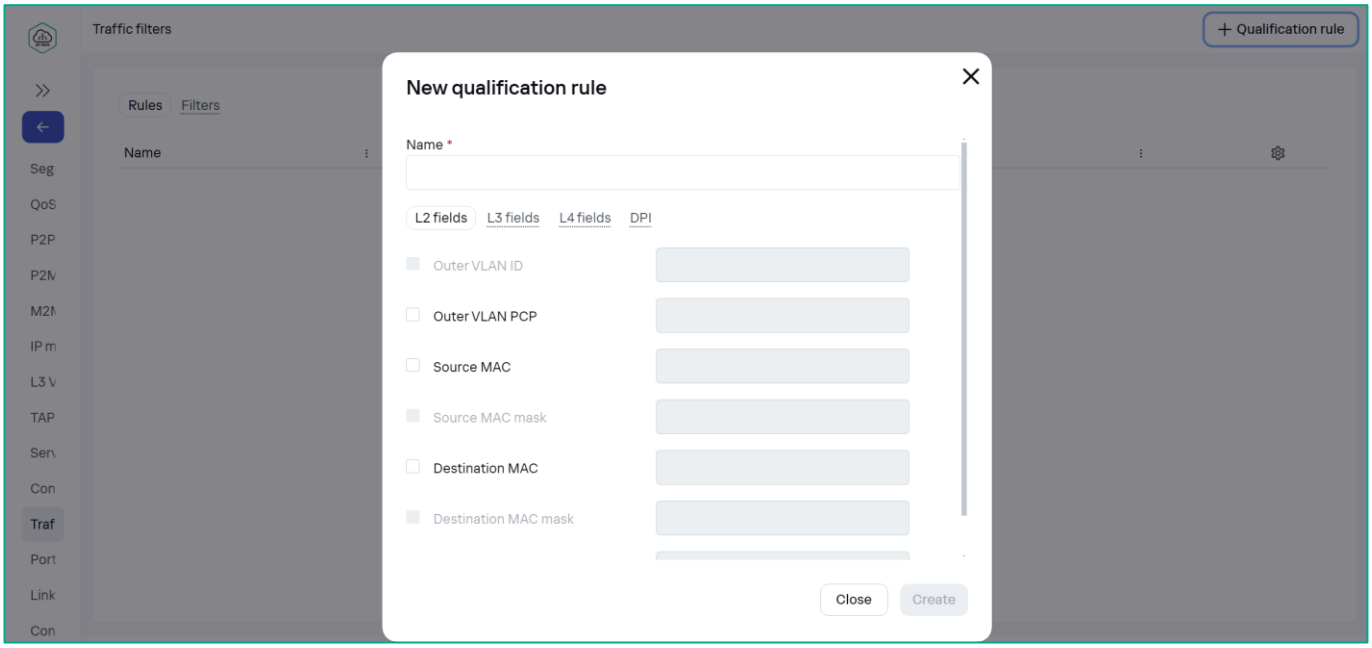
Нажать **Create**

Данное пороговое ограничение исключит из путей прохождения трафика линки, для которых задан параметр Last resort.

3.6.5. Создать правило для классификации тестового трафика

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

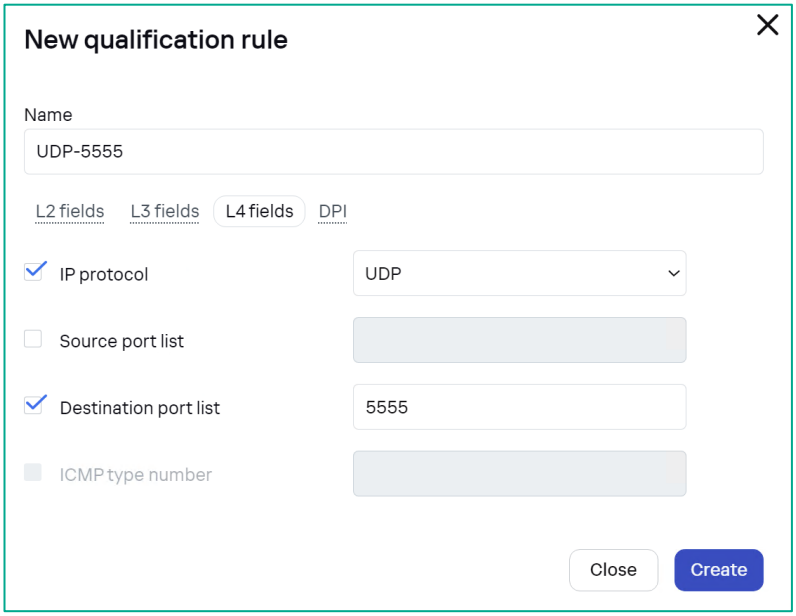
Перейти в меню **Traffic Filters**. Затем открыть вкладку **Rules** и нажать **+ Qualification rule**



Задать параметры правила:

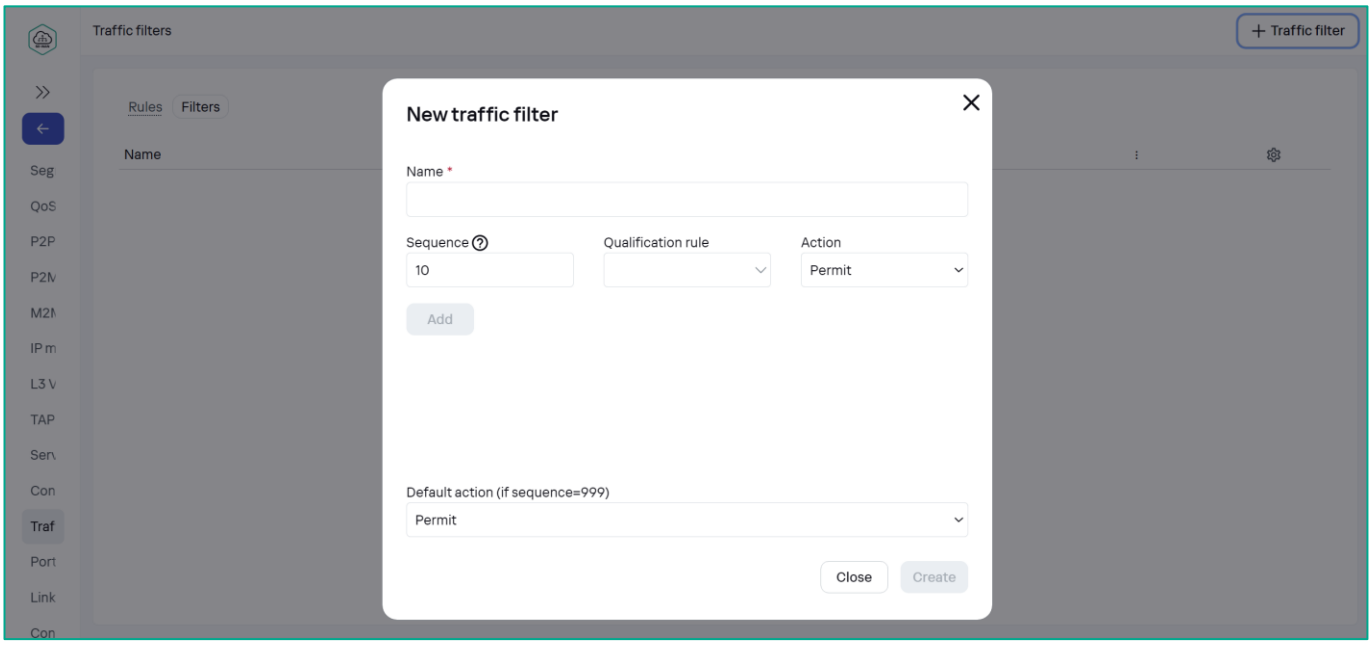
- Название правила (в примере **UDP-5555**)
- **L3 Fields**:
  - **Protocol**: **IPv4**
- **L4 Fields**:
  - **IP protocol**: **UDP**
  - **Destination port list**: **5555**

Нажать **Create**



3.6.6. Создать фильтр для направления тестового трафика в отдельный сервис.

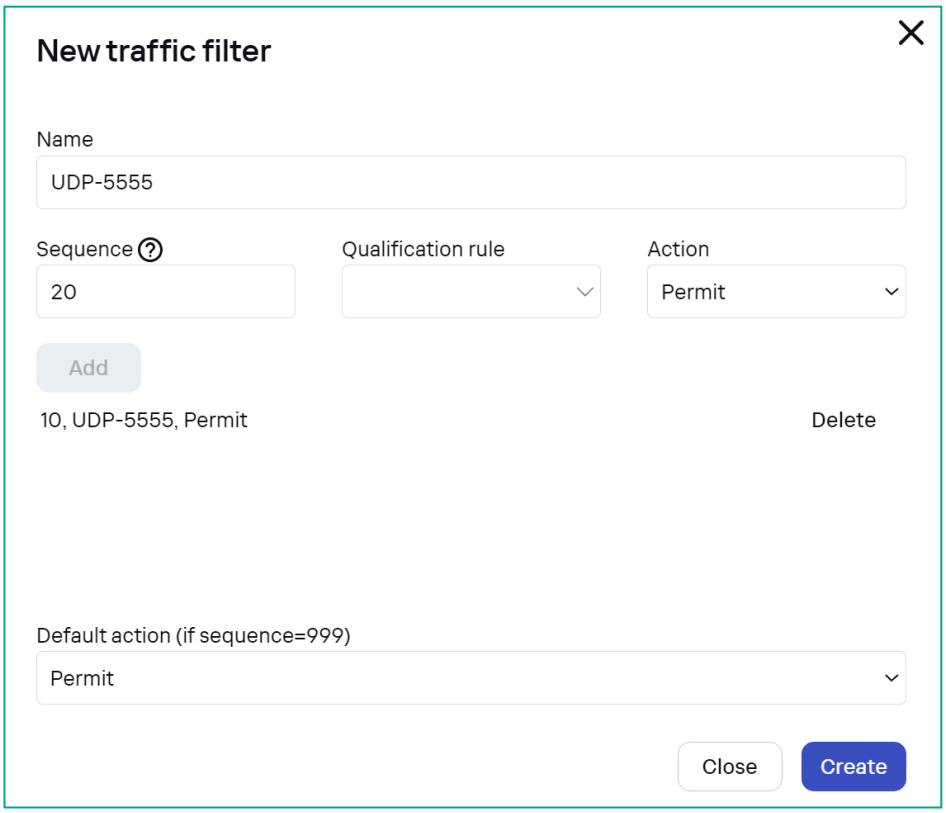
Перейти на вкладку **Filters**, нажать **+ Traffic filter**



Задать параметры фильтра:

- Название (в примере **UDP-5555**)
- Добавить правило классификации: выбрать в селекторе **Qualification rule** созданное в п. 3.6.5, задать **Action**: **Permit**. Нажать **Add**

Нажать **Create**



3.6.7. Создать сервисные интерфейсы типа ACL.

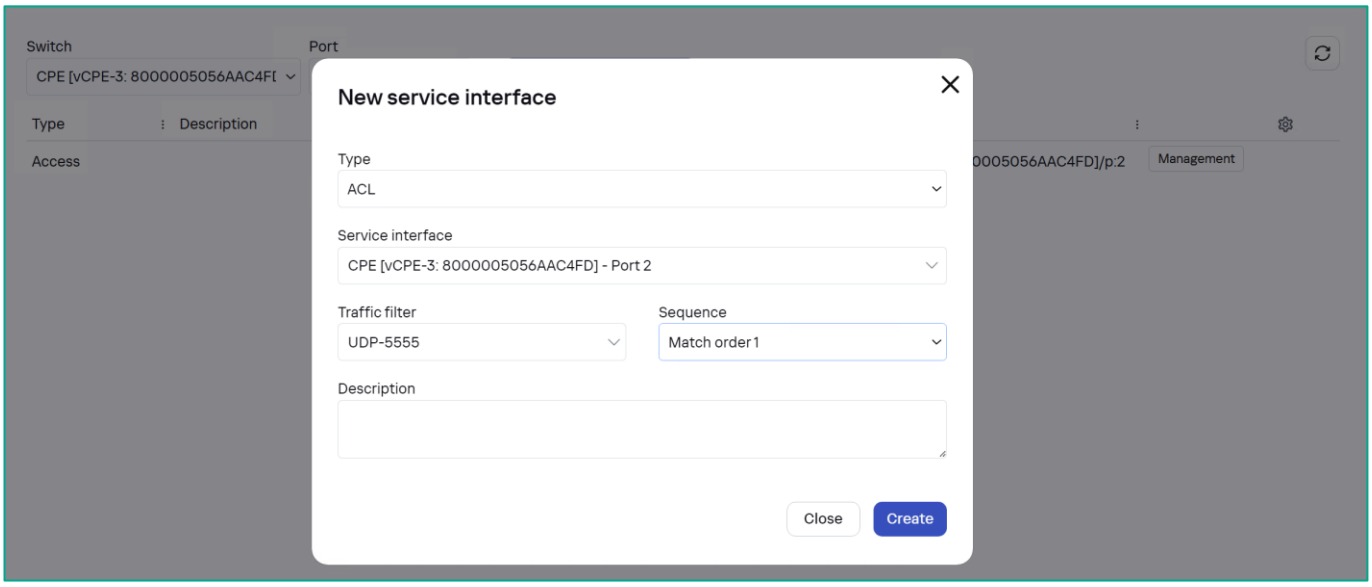
Трафик попадает в транспортный сервис через сервисные интерфейсы. Необходимо создать специальный ACL интерфейс (ACL Service Interface – ACL SI). Перейти в меню **Service Interfaces**, затем выбрать **Switch**: **vCPE-3** и **Port**: **2 (ovs-lan)**

Нажать **Create service interface**

Задать параметры сервисного интерфейса:

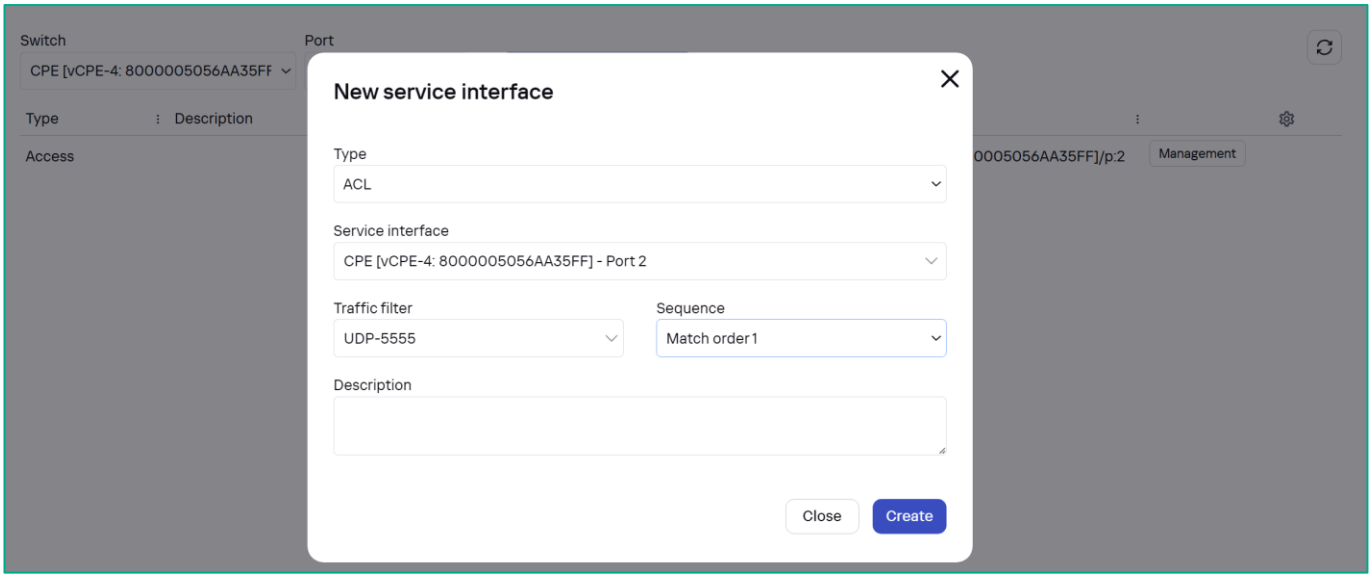
- **Type**: **ACL**
- **Service interface: vCPE-3** - **Port 2**
- **Traffic Filter** для UDP 5555, созданный в пункте 3.6.6
- **Sequence**: **Match order 1** (данный ACL SI будет первым обрабатывать трафик)

Нажать **Create**



При создании сервиса требуется создать сервисные интерфейсы для каждой CPE.

Создать аналогичный ACL сервисный интерфейс для **vCPE-4**.



3.6.8. Создать отдельный транспортный сервис для приоритетного трафика.

Перейти в меню **M2M Services**, нажать **+ M2M service**

Задать параметры сервиса:

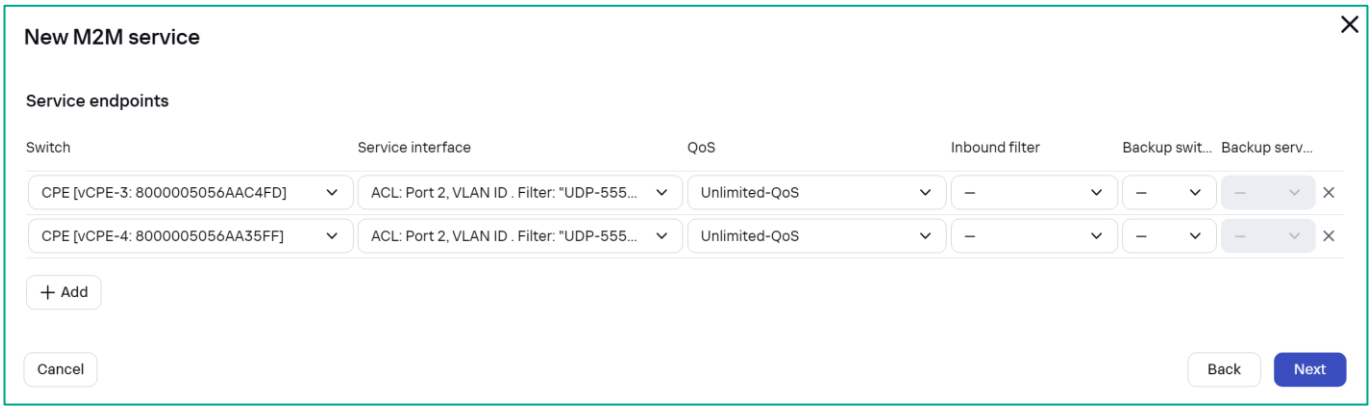
- Название (в примере **M2M_ACL**)
- **Constraint**: созданное в пункте 3.6.4 пороговое ограничение **(threshold)**

Нажать **Next**

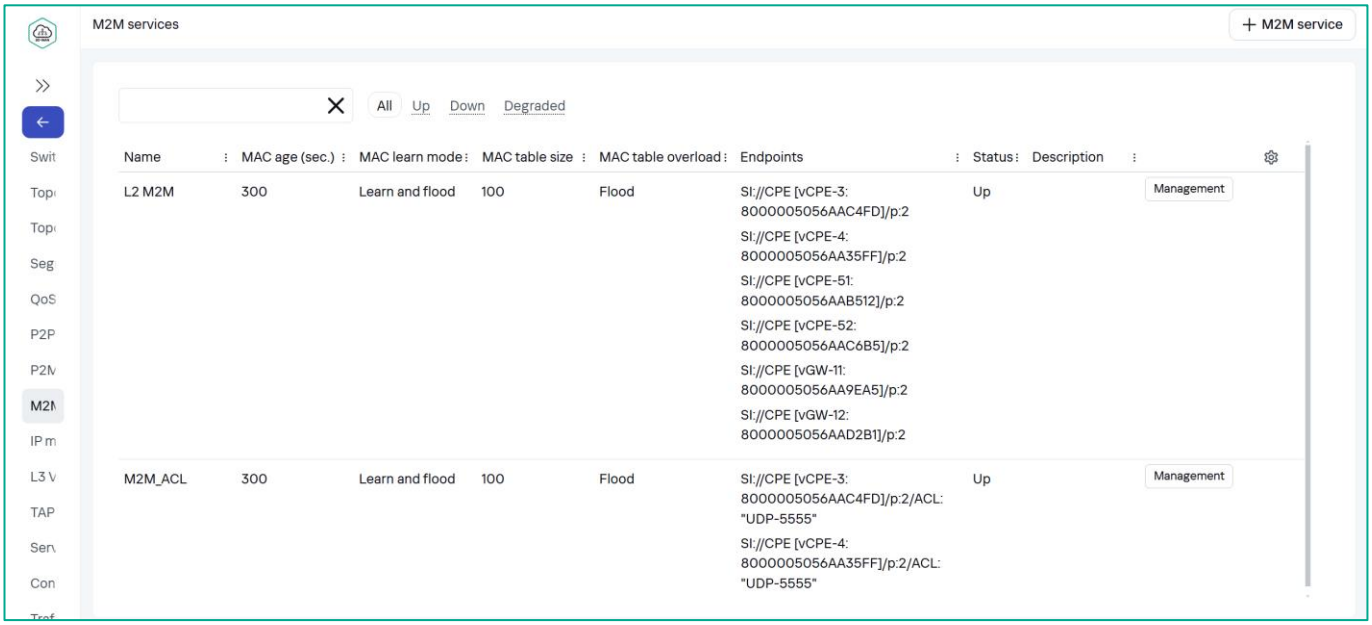
В секции **Service endpoints** нажать **+ Add** и добавить сервисные интерфейсы, созданные в п. 3.6.7.

Задать параметры **service endpoints**:

- **Switch**: **vCPE-3** и **vCPE-4**
- **Service interface**: Созданные в п. 3.6.7 **ACL Service Interfaces**
- **QoS**: **Unlimited QoS**



Нажать **Next** и **Create**



3.6.9. Проверить работу приоритезации трафика в отдельный транспортный сервис.

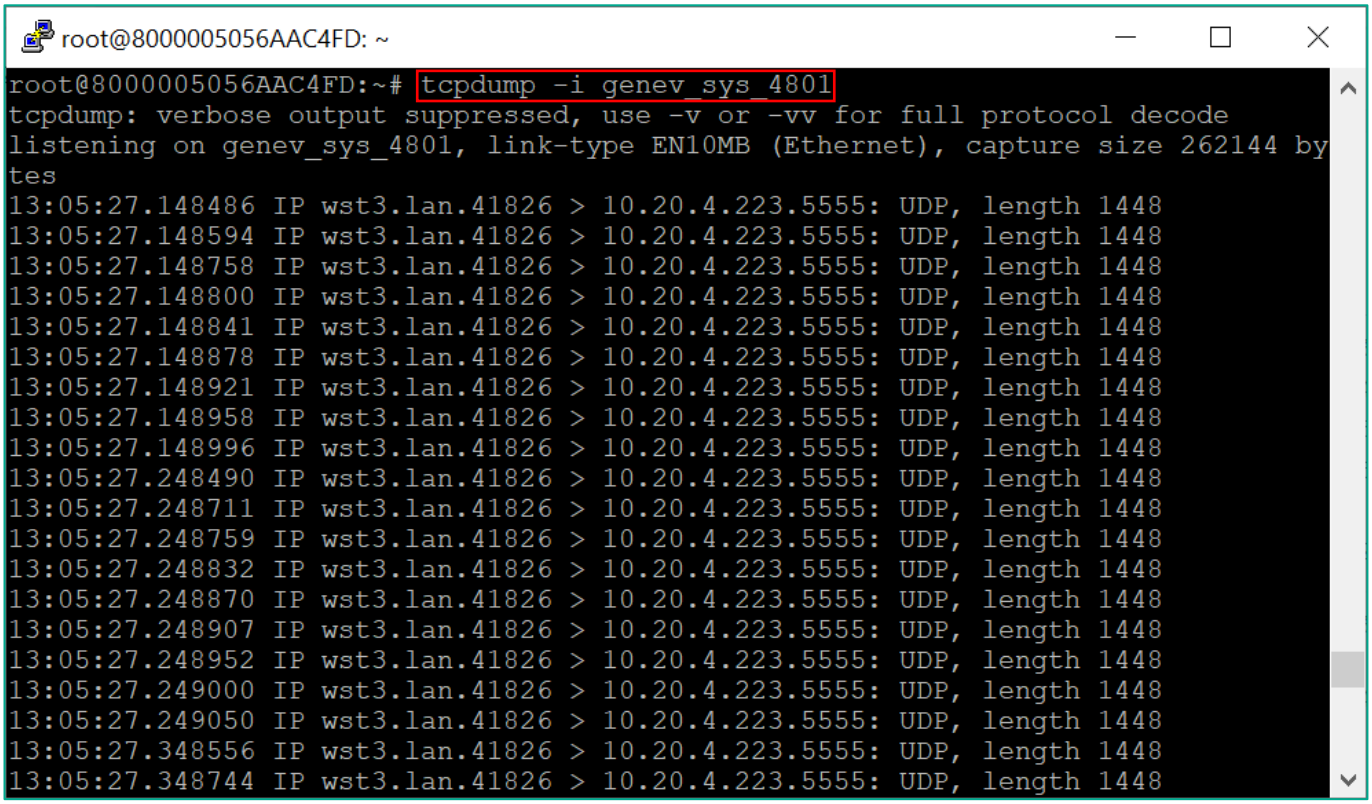
Подключиться к vCPE-3 по SSHи проверить, что трафик переключился на другой WAN интерфейс (в зависимости от настроек, сделанных ранее).

В пункте 3.6.2 проверялось, что трафик идёт через туннельный 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).



3.6.10. Вернуть настройки после завершения теста.

Удалить сервис, созданный в п. 3.6.8 (при удалении отметить **Delete associated service interfaces**).

Убрать параметр **Last resort** с линков, добавленный в п. 3.6.3.

Остановить **iperf** на **wst3** и **wst4**, 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:

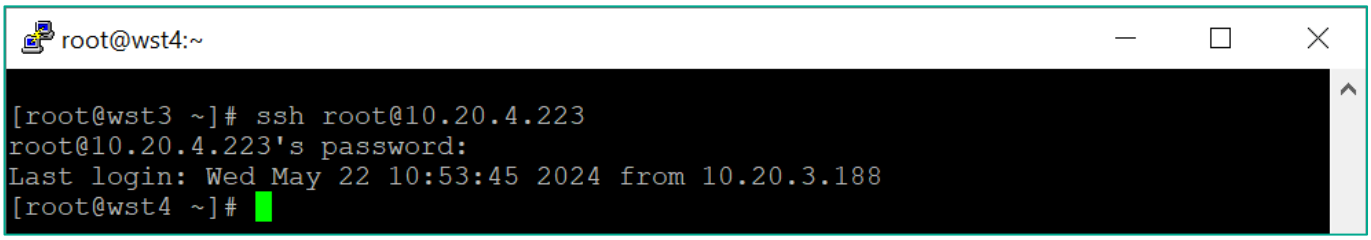
https://support.kaspersky.com/help/SD-WAN/2.3/ru-RU/246544.htm

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

3.7.1. Сгенерировать тестовый трафик между wst3 и wst4.

Запустить сессию SSH на хосте **wst3** до **wst4**:

```
ssh root@<wst4 IP address>
```



3.7.2. Проверить, через какой туннельный интерфейс отправляется тестовый трафик.

Подключиться к **vCPE-3** по SSH и запустить **tcpdump** для отображения пакетов, проходящих через туннельный интерфейс **genev_sys_4800**:

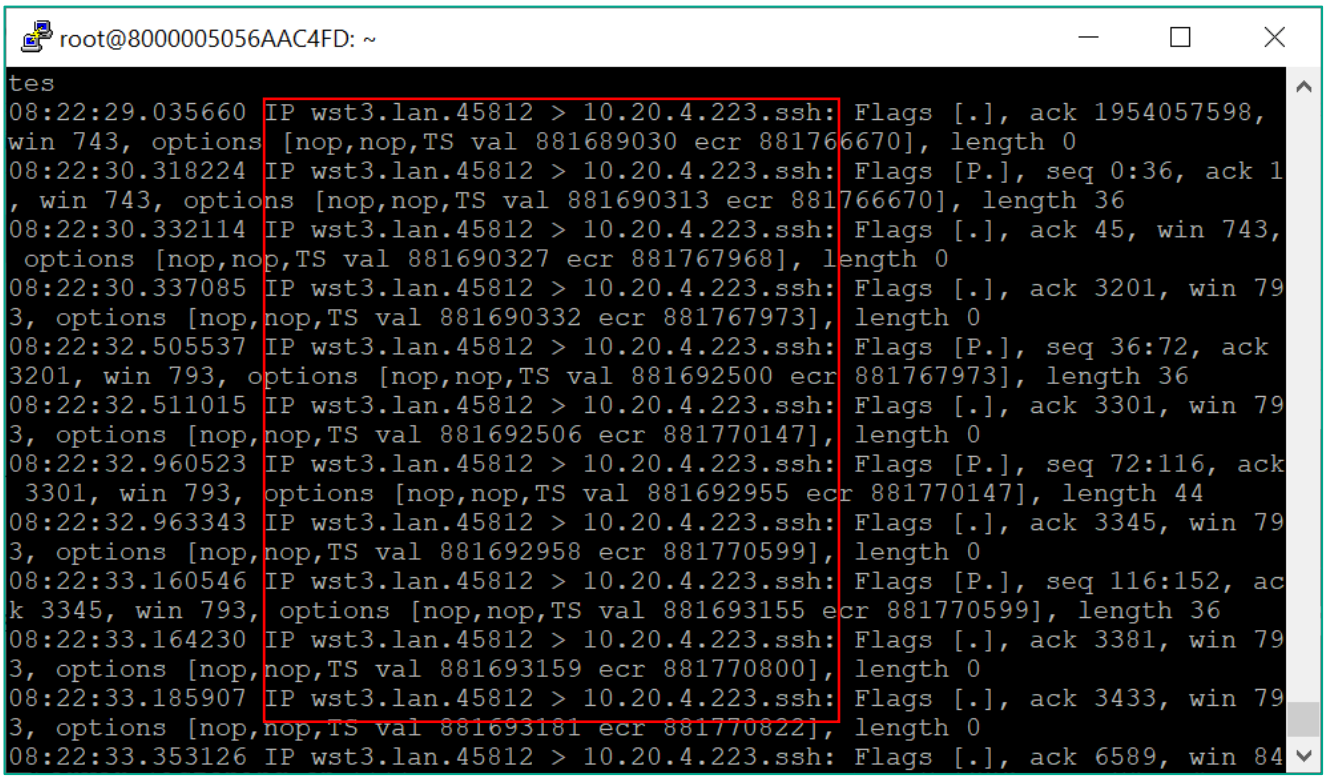
```
tcpdump -i genev_sys_4800
```

Если тестовый трафик проходит через туннельный интерфейс, то в выводе **tcpdump** будут видны пакеты **ssh**, отправленные от **wst3** до **wst4**.

Определить по выводу tcpdump через какой интерфейс проходит тестовый трафик: **genev_sys_4800** или **genev_sys_4801**. Для SSH сессии трафик может идти ассиметрично (в одну сторону через 4800, а в другую через 4801).

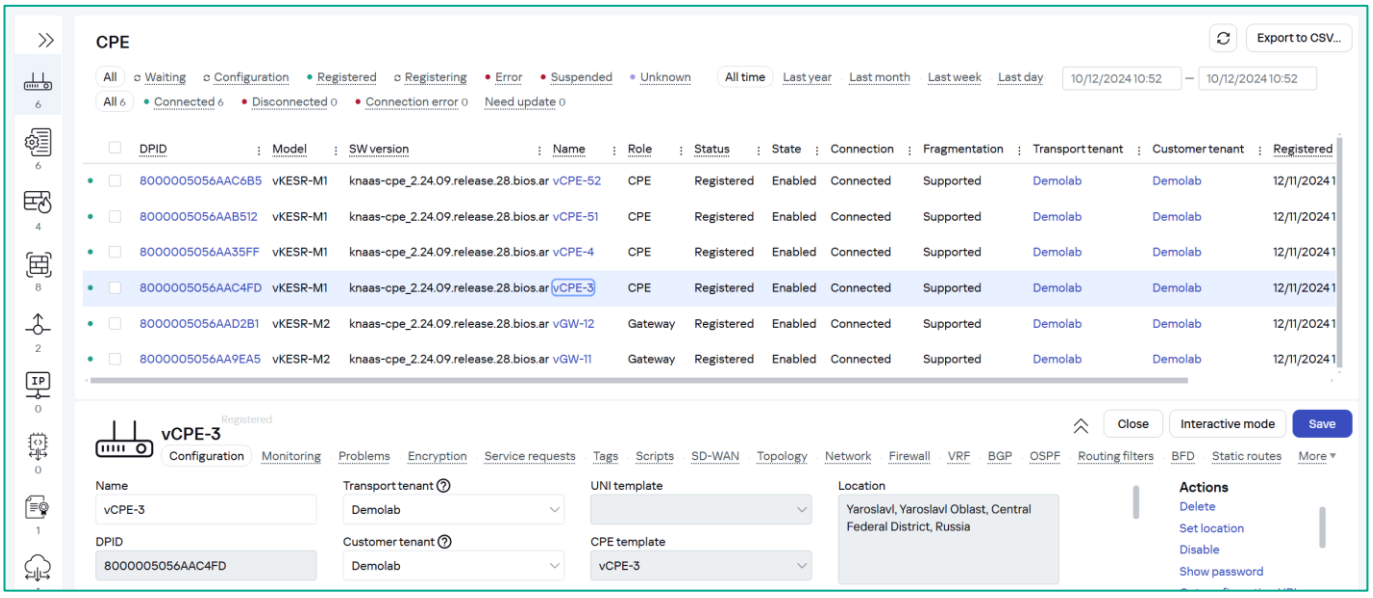
genev_sys – туннельные интерфейсы CPE. Номер порта указывает на номер WAN интерфейса CPE устройства. Номера назначаются по порядку, начиная с порта 4800, по одному на каждый WAN интерфейс. Порт **4800** означает WAN интерфейс **sdwan0** (eth0), порт **4801** означает WAN интерфейс **sdwan1** (eth1).

В данном примере трафик проходит через интерфейс **genev_sys_4800**.

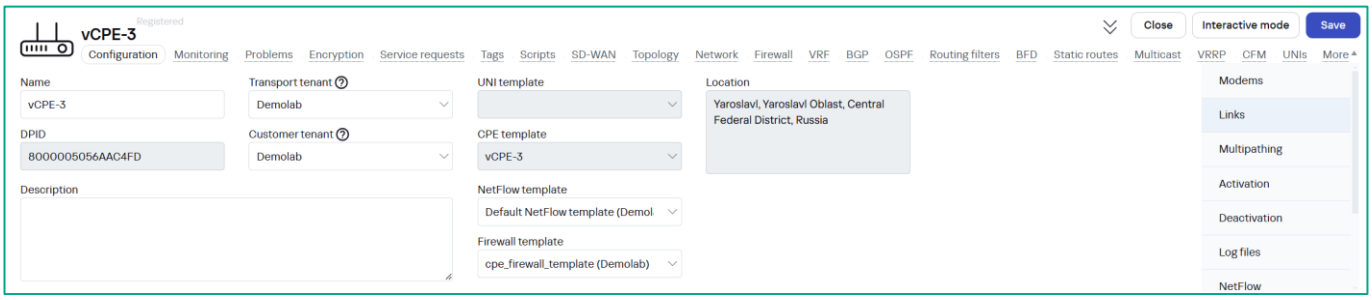


3.7.3. Задать параметр Last resort для линков vCPE-3.

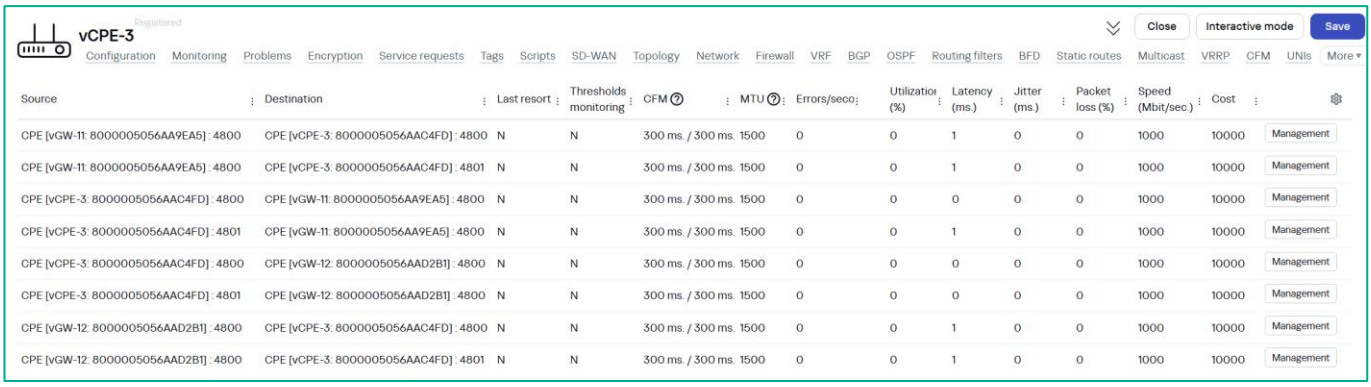
Перейти в меню **CPE** и выбрать **vCPE-3**.



Перейти на вкладку **Links**.



Отобразится список построенных линков с **vCPE-3**.



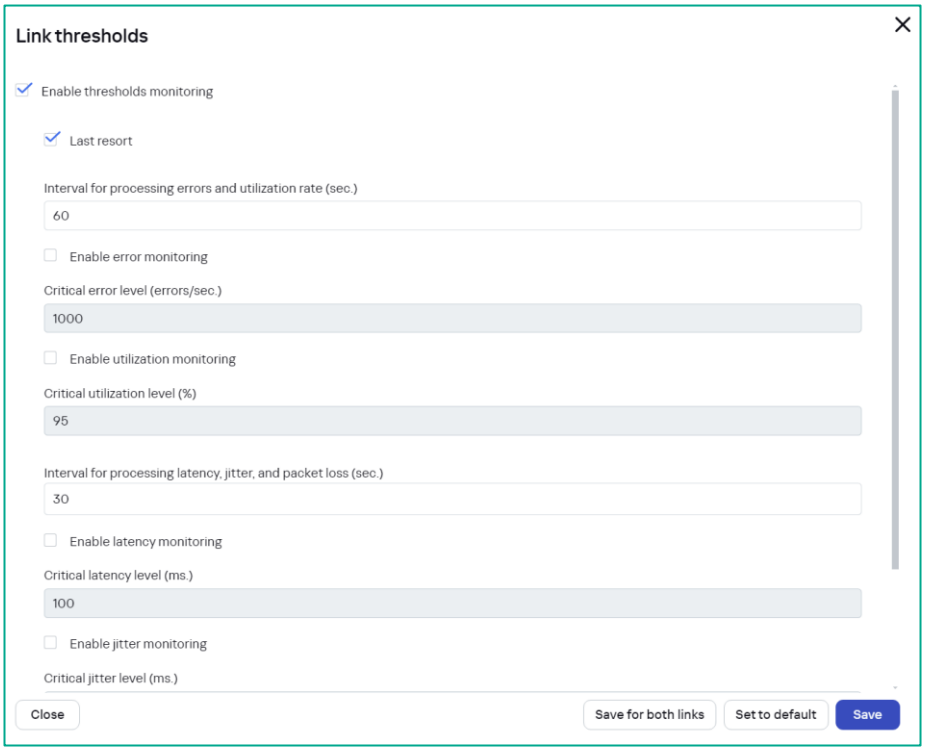
Найти все линки, через которые проходит трафик: порты источника или назначения линков (4800 или 4801) должны совпадать с номером туннельного интерфейса CPE согласно проверке в пункте 3.7.2. В данном примере трафик проходит через интерфейс **genev_sys_4800**

Линки, через которые проходит трафик в данном 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**

Для всех найденных линков поочередно нажать **Management → Set thresholds** и задать параметр **Last resort** для линков:

- Отметить **Enable tunnel thresholds monitoring**
- Отметить **Last resort**

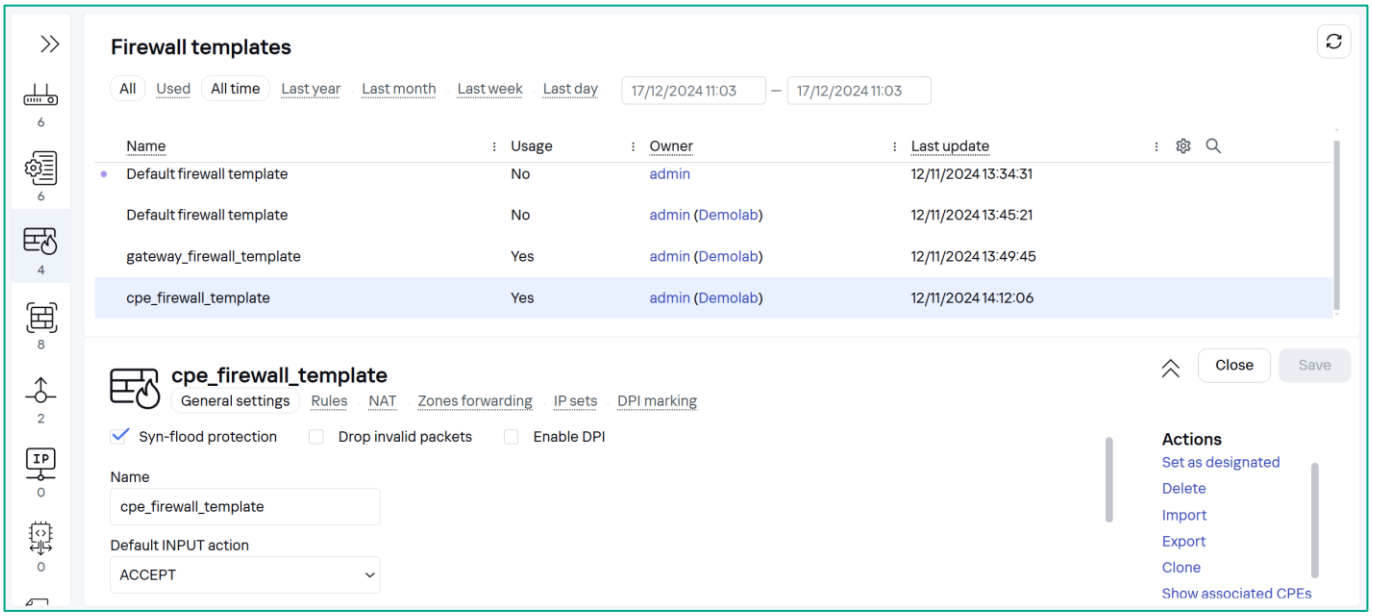


Нажать **Save for both links** – сохранение параметров мониторинга линков в оба направления.

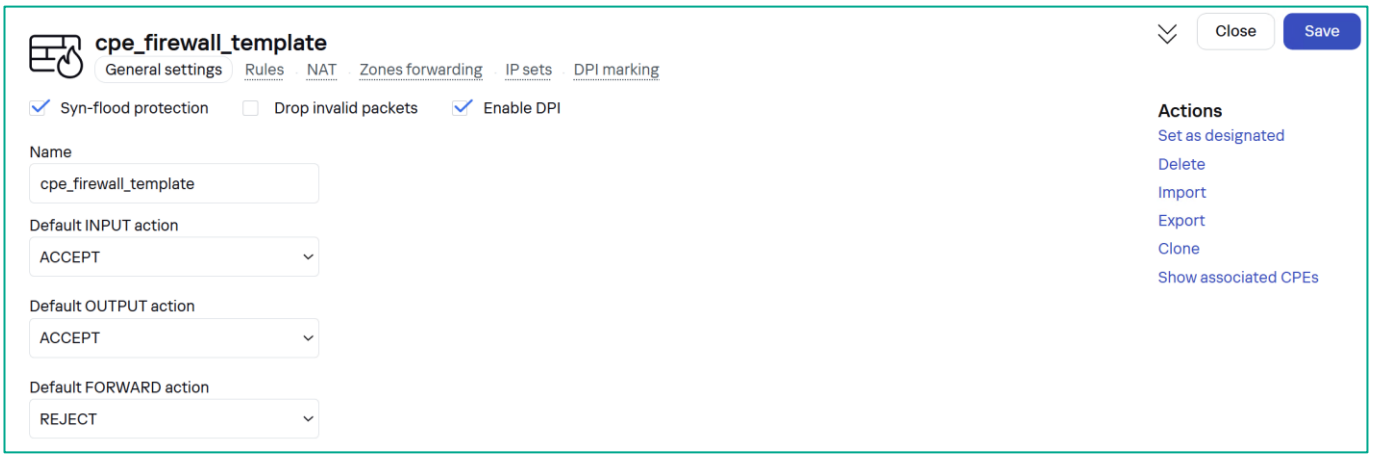
3.7.4. Включить DPI в шаблоне межсетевого экрана CPE.

Для работы DPI требуется изменить настройки межсетевого экрана.

Перейти меню **Firewall templates** и открыть шаблон **cpe_firewall_template**, применённый к vCPE-3 и vCPE-4.

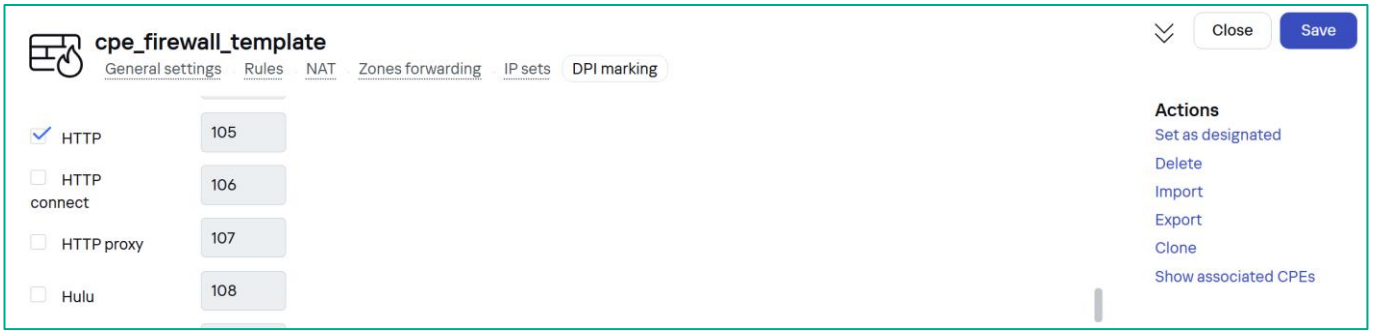


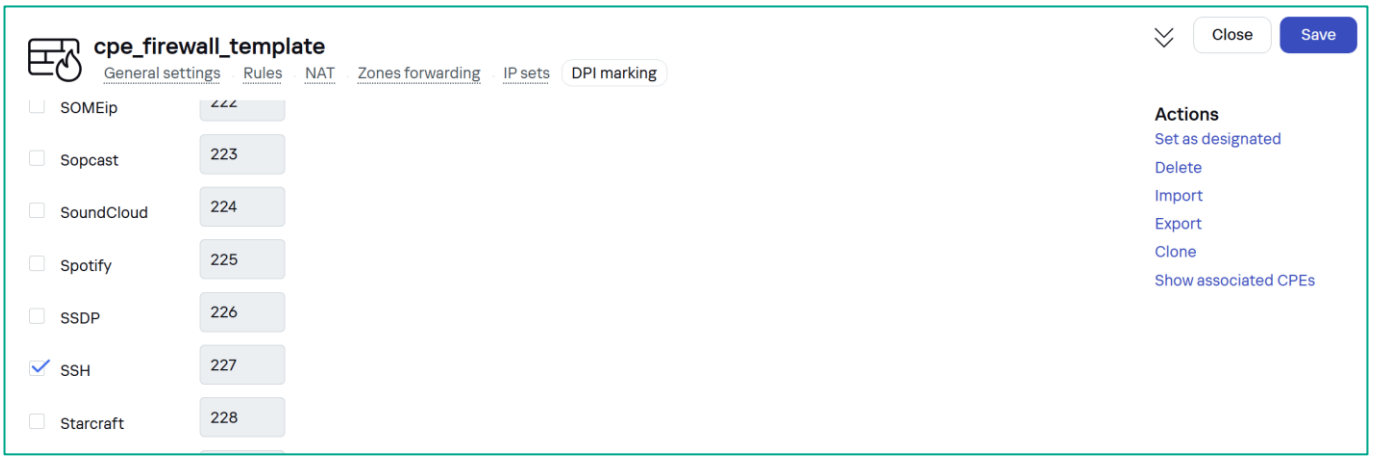
На вкладке General settings отметить **Enable DPI**



На вкладке **DPI marking** отметить протоколы, которые будут определяться DPI:

- **HTTP**
- **SSH**



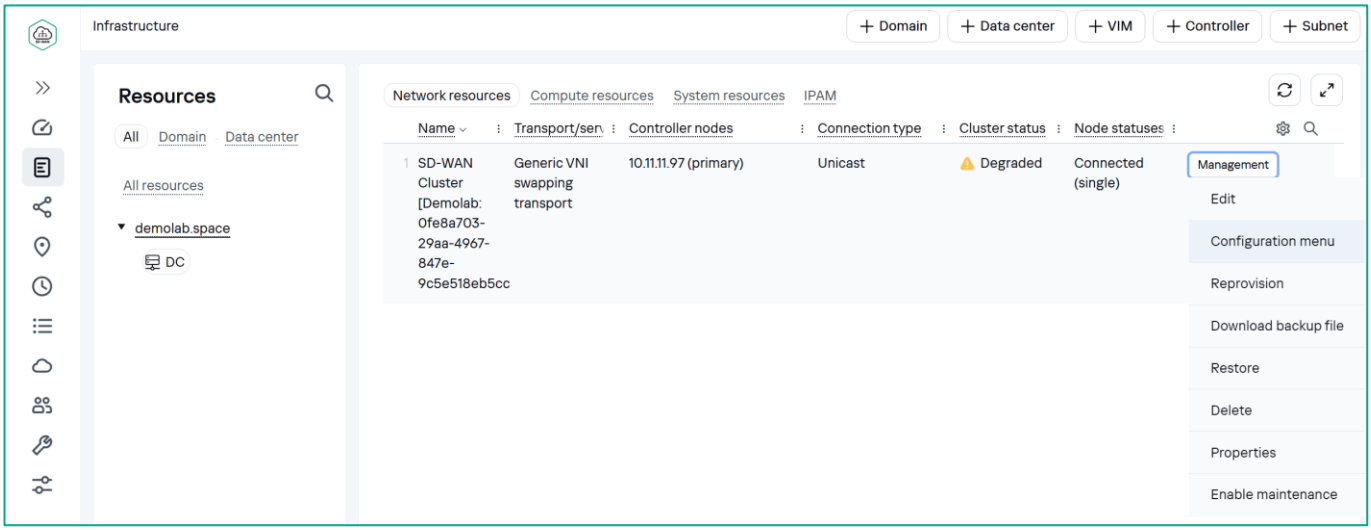


Нажать **Save**

3.7.5. Создать пороговое ограничение для исключения линков с параметром Last resort.

Для перенаправления трафика необходимо создать пороговые ограничения (**Constraints**).

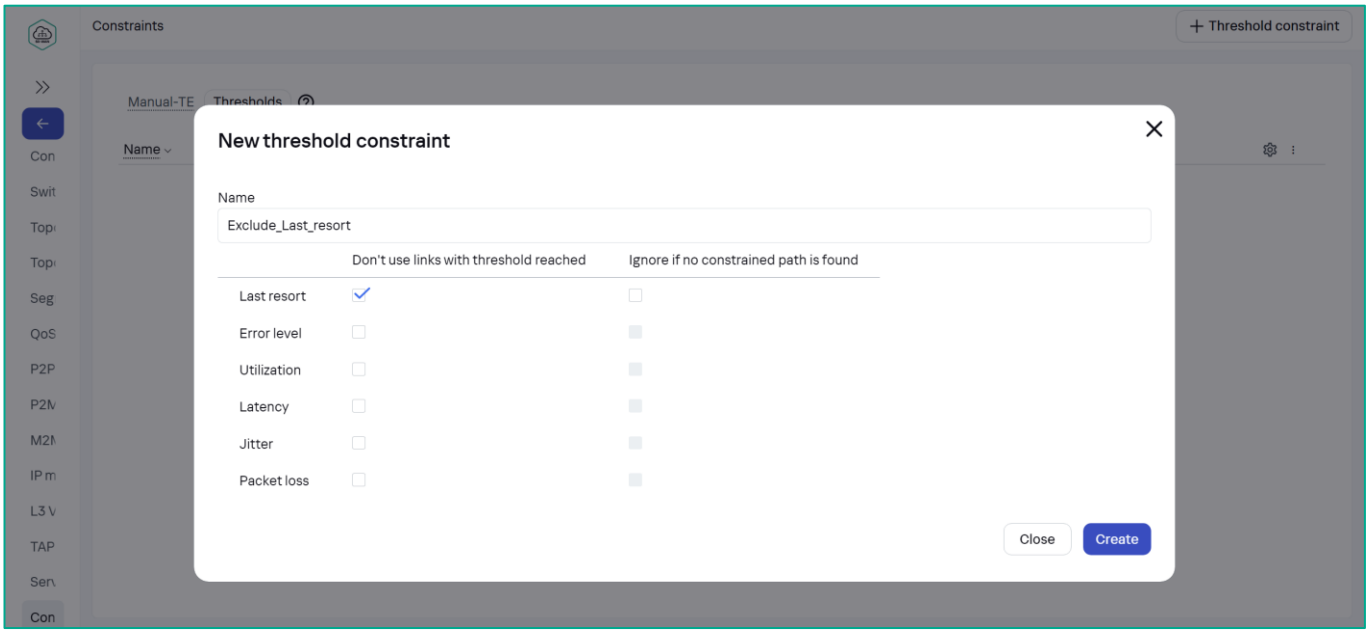
Перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu**



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

Задать параметры порогового ограничения:

- Название (в примере **Exclude_Last_resort**)
- Отметить ограничение для **Last resort**



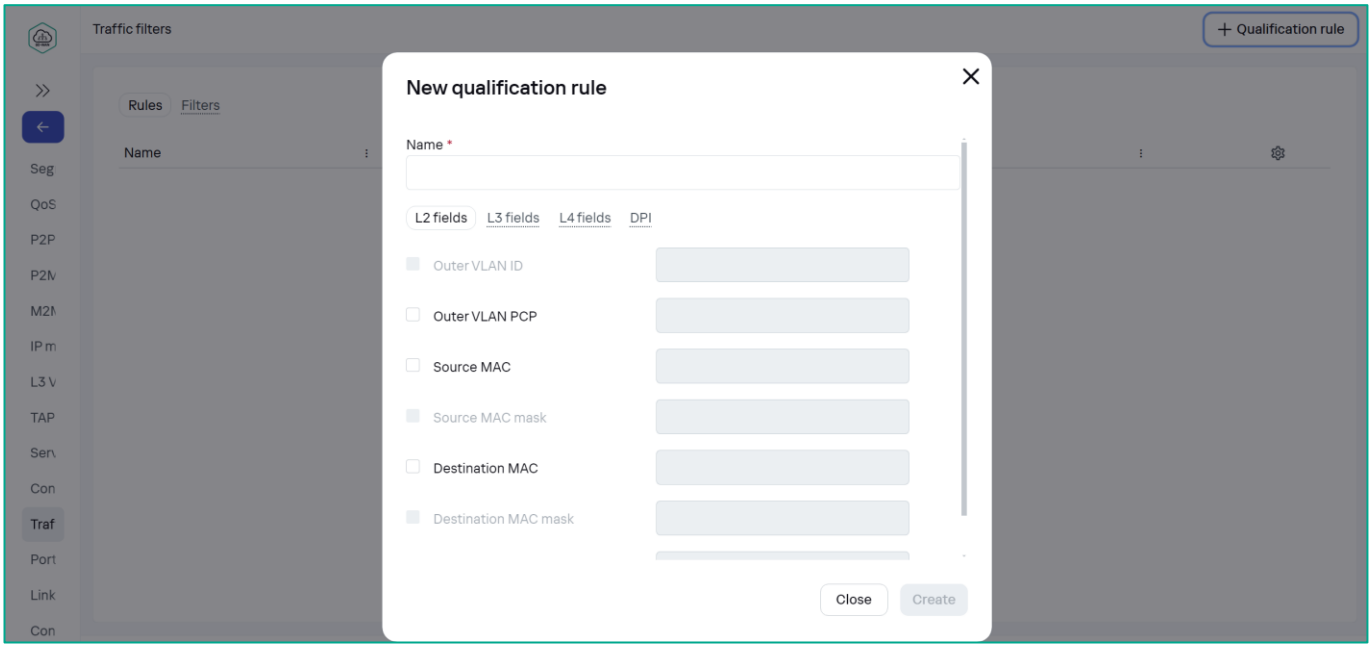
Нажать **Create**

Данное пороговое ограничение исключит из путей прохождения трафика линки, для которых задан параметр Last resort.

3.7.6. Создать правило для классификации тестового трафика SSH.

Для направления трафика в отдельный сервис нужно создать список доступа ACL с правилами классификатора DPI.

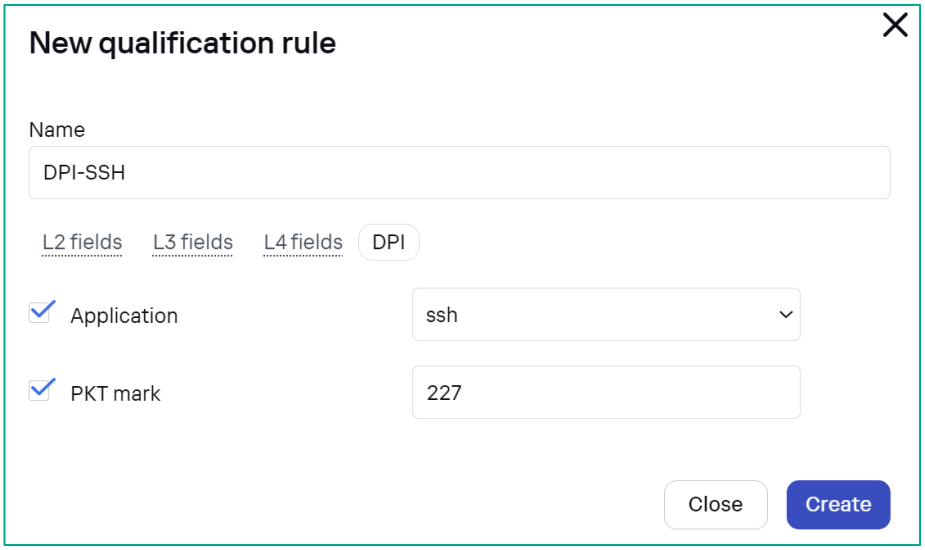
Перейти в меню **Traffic Filters**. Затем открыть вкладку **Rules** и нажать **+ Qualification rule**



Задать параметры правила:

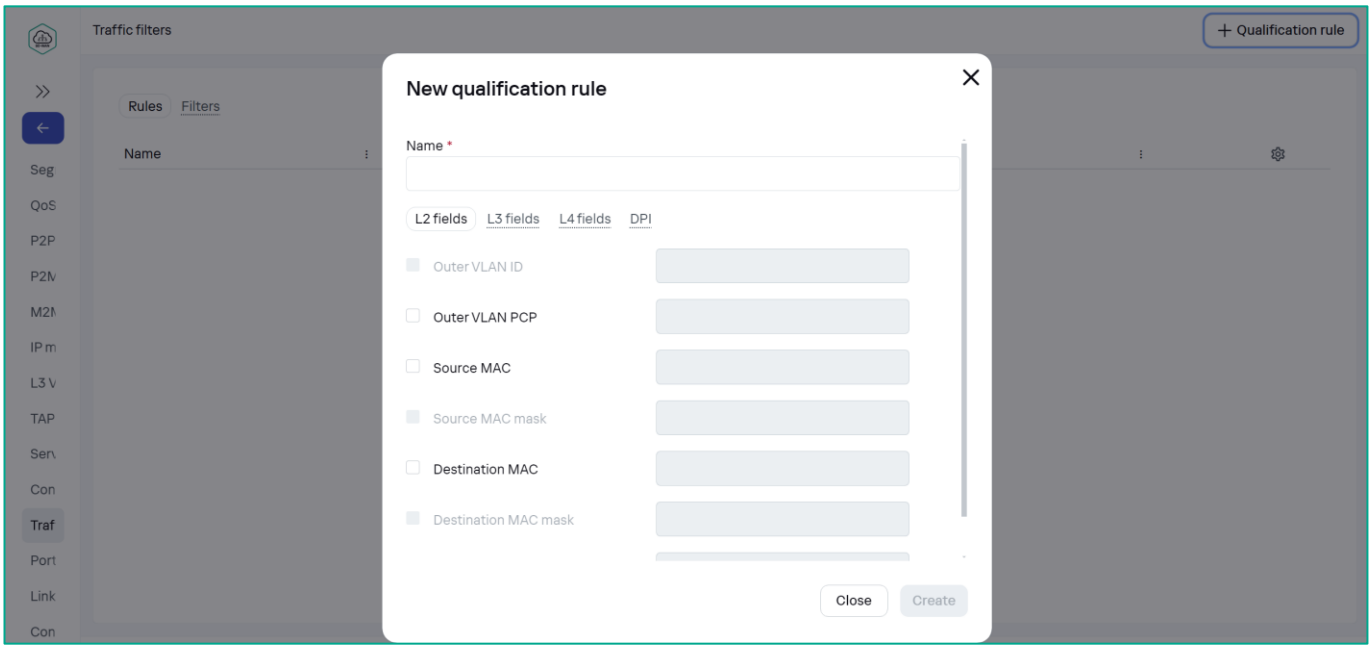
- Название правила (в примере **DPI-SSH**)
- **L3 Fields**:
  - **Protocol**: **IPv4**
- **DPI**:
  - **Application**: **ssh**

Нажать **Create**



3.7.7. Создать правило для классификации тестового трафика HTTP.

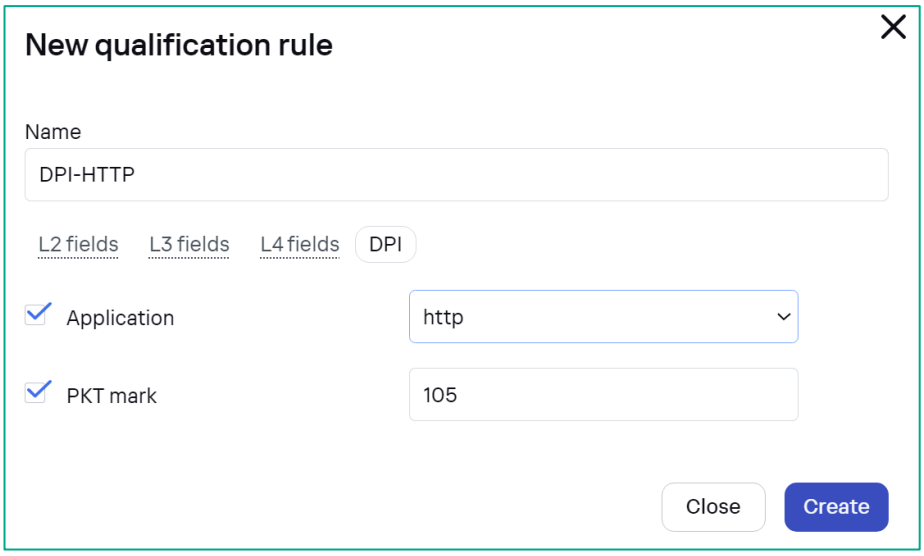
Перейти в меню **Traffic Filters**. Затем открыть вкладку **Rules** и нажать **+ Qualification rule**



Задать параметры правила:

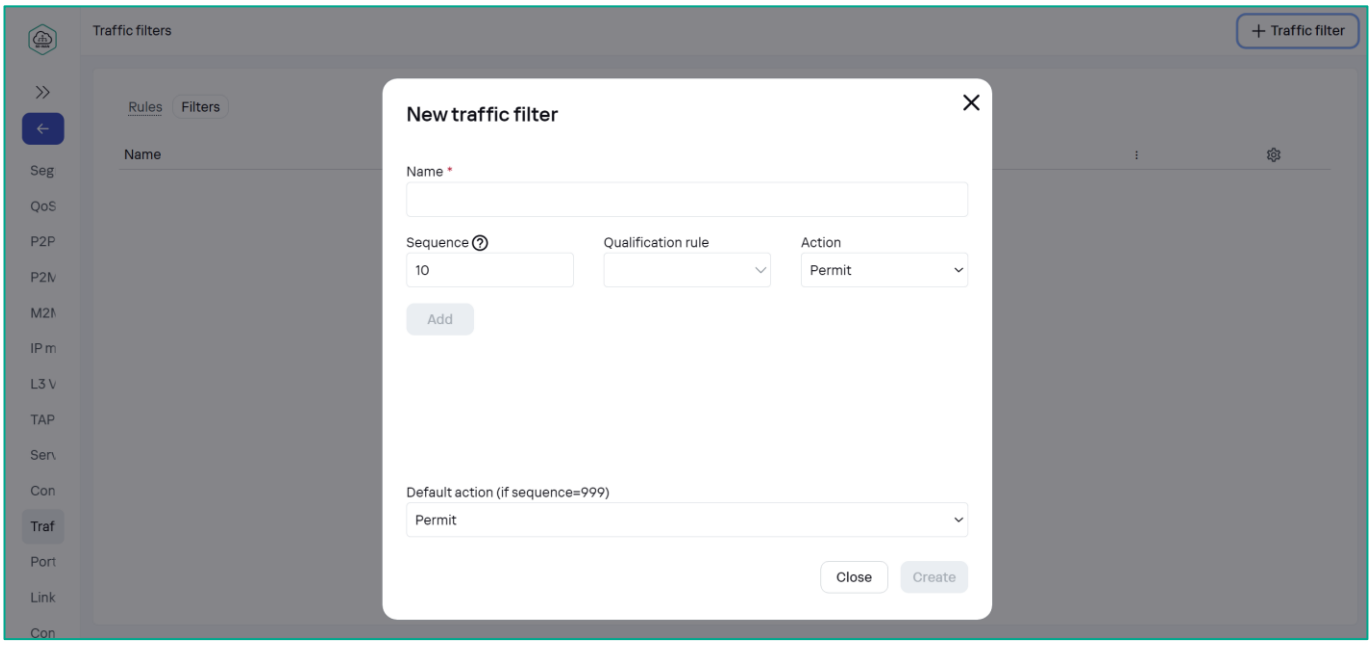
- Название правила (в примере **DPI-HTTP**)
- **L3 Fields**:
  - **Protocol**: **IPv4**
- **DPI**:
  - **Application**: **http**

Нажать **Create**



3.7.8. Создать фильтр для направления тестового трафика в отдельный сервис.

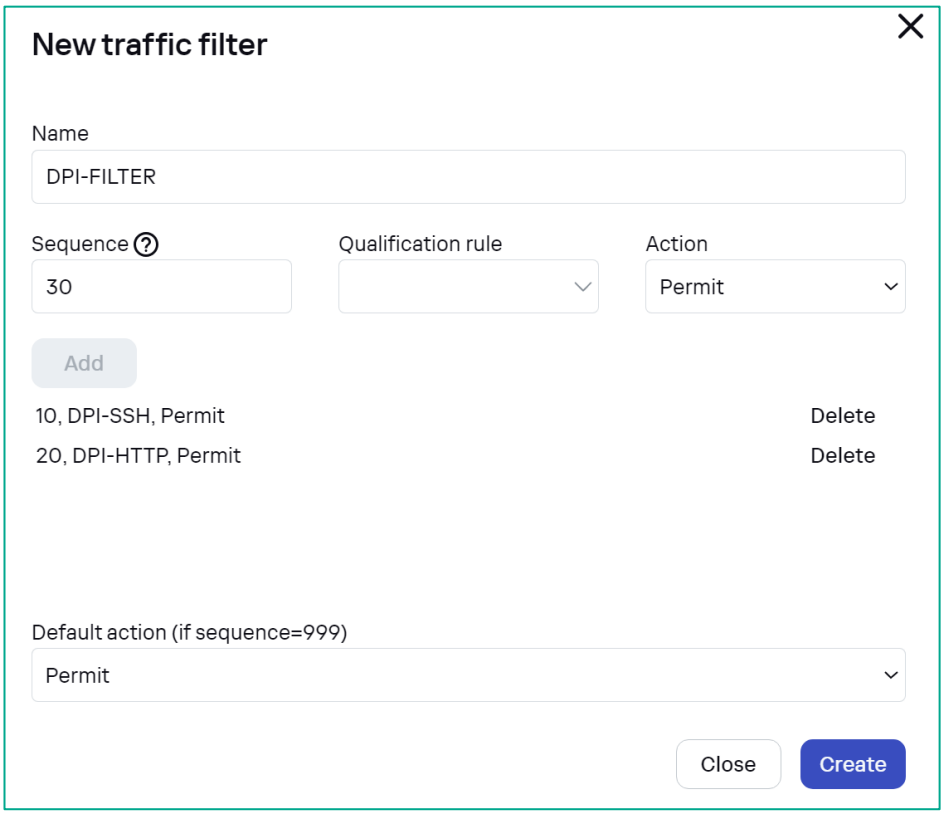
Перейти на вкладку **Filters**, нажать **+ Traffic filter**



Задать параметры фильтра:

- Название (в примере **DPI-FILTER**)
- Добавить правила классификации: выбрать в селекторе **Qualification rule** созданные в п. 3.7.6 и 3.7.7, задать **Action**: **Permit**. Нажать **Add**

Нажать **Create**



3.7.9. Создать сервисные интерфейсы типа ACL.

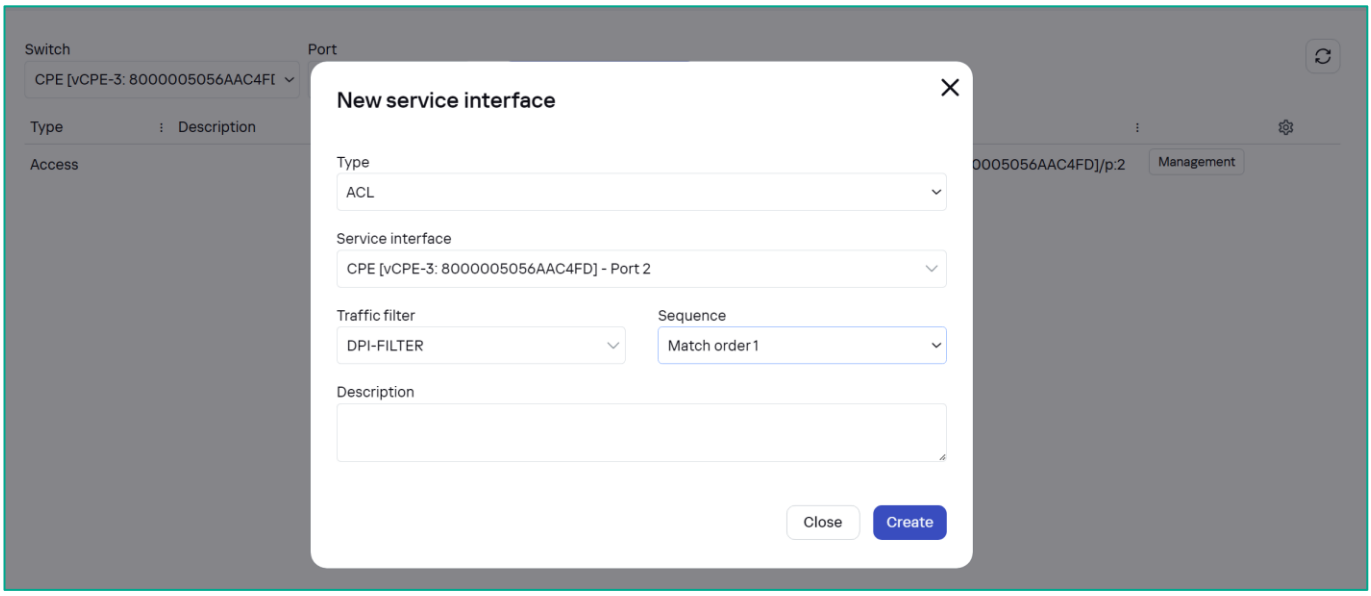
Трафик попадает в транспортный сервис через сервисные интерфейсы. Необходимо создать специальный ACL интерфейс (ACL Service Interface – ACL SI). Перейти в меню **Service Interfaces**, затем выбрать **Switch**: **vCPE-3** и **Port**: **2 (ovs-lan)**

Нажать **Create service interface**

Задать параметры сервисного интерфейса:

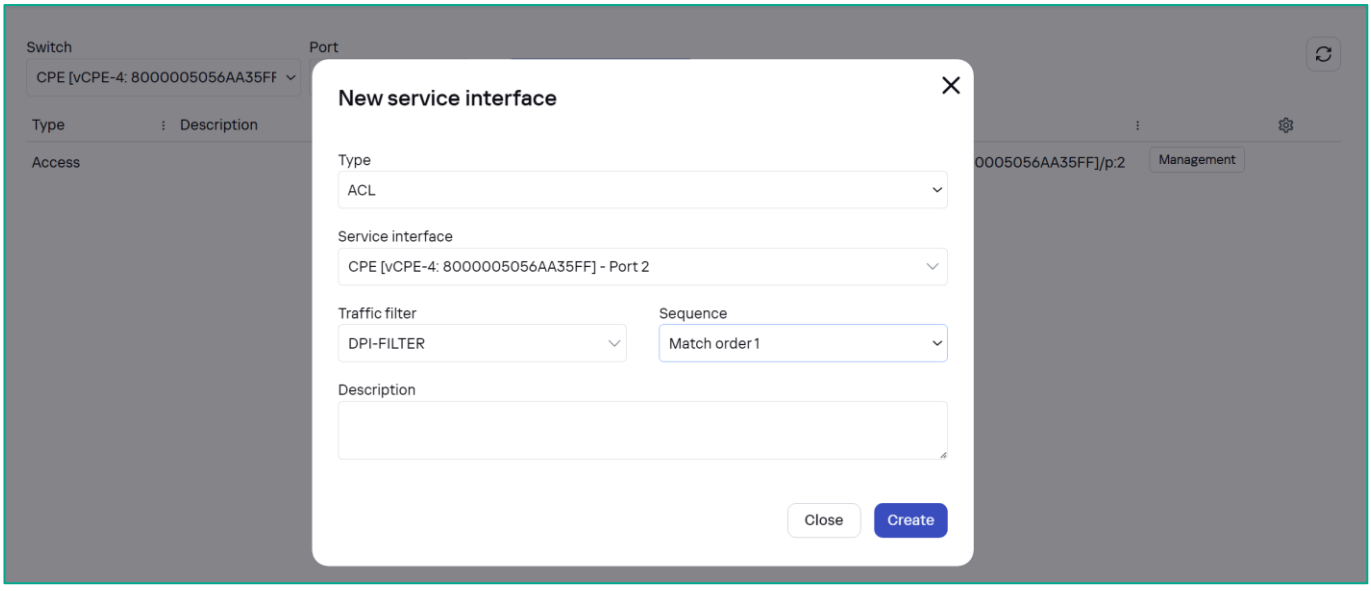
- **Type**: **ACL**
- **Service interface: vCPE-3** - **Port 2**
- **Traffic Filter** с классификаторами DPI, созданный в пункте 3.7.8
- **Sequence**: **Match order 1** (данный ACL SI будет первым обрабатывать трафик)

Нажать **Create**



При создании сервиса требуется создать сервисные интерфейсы для каждой CPE.

Создать аналогичный ACL сервисный интерфейс для **vCPE-4**.



3.7.10. Создать отдельный транспортный сервис для приоритетного трафика.

Перейти в меню **M2M Services**, нажать **+ M2M service**

Задать параметры сервиса:

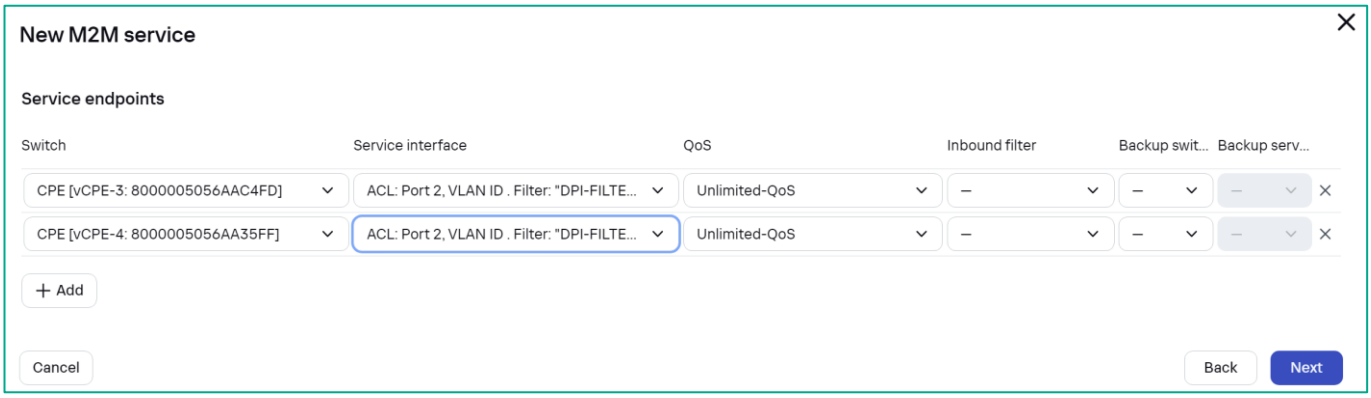
- Название (в примере **M2M_ACL**)
- **Constraint**: созданное в пункте 3.7.5 пороговое ограничение **(threshold)**

Нажать **Next**

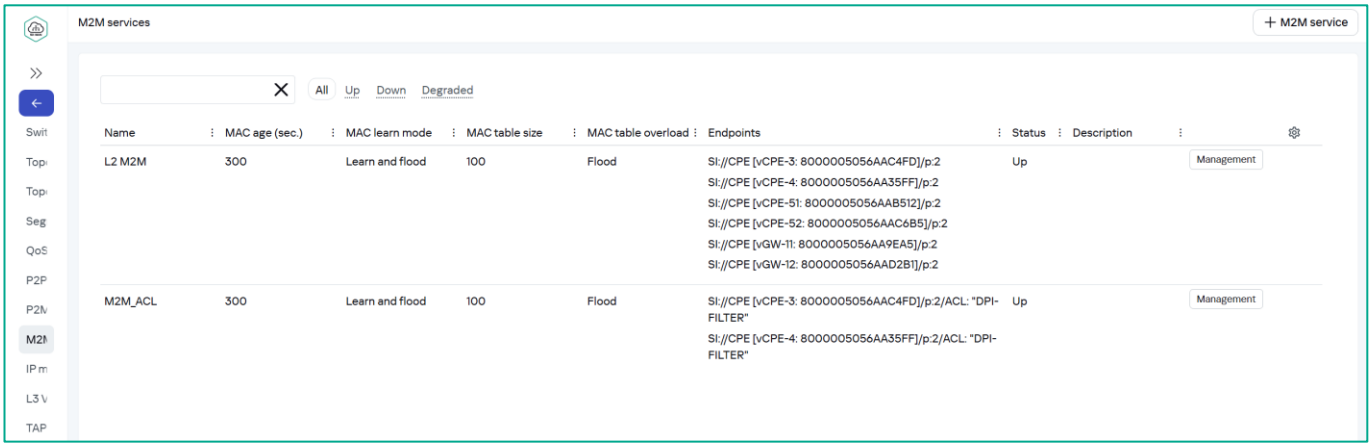
В секции **Service endpoints** нажать **+ Add** и добавить сервисные интерфейсы, созданные в п. 3.7.9.

Задать параметры **service endpoints**:

- **Switch**: **vCPE-3** и **vCPE-4**
- **Service interface**: Созданные в п. 3.7.9 ACL Service interfaces
- **QoS**: **Unlimited QoS**



Нажать **Next** и **Create**



3.7.11. Проверить работу приоритезации SSH трафика в отдельный транспортный сервис.

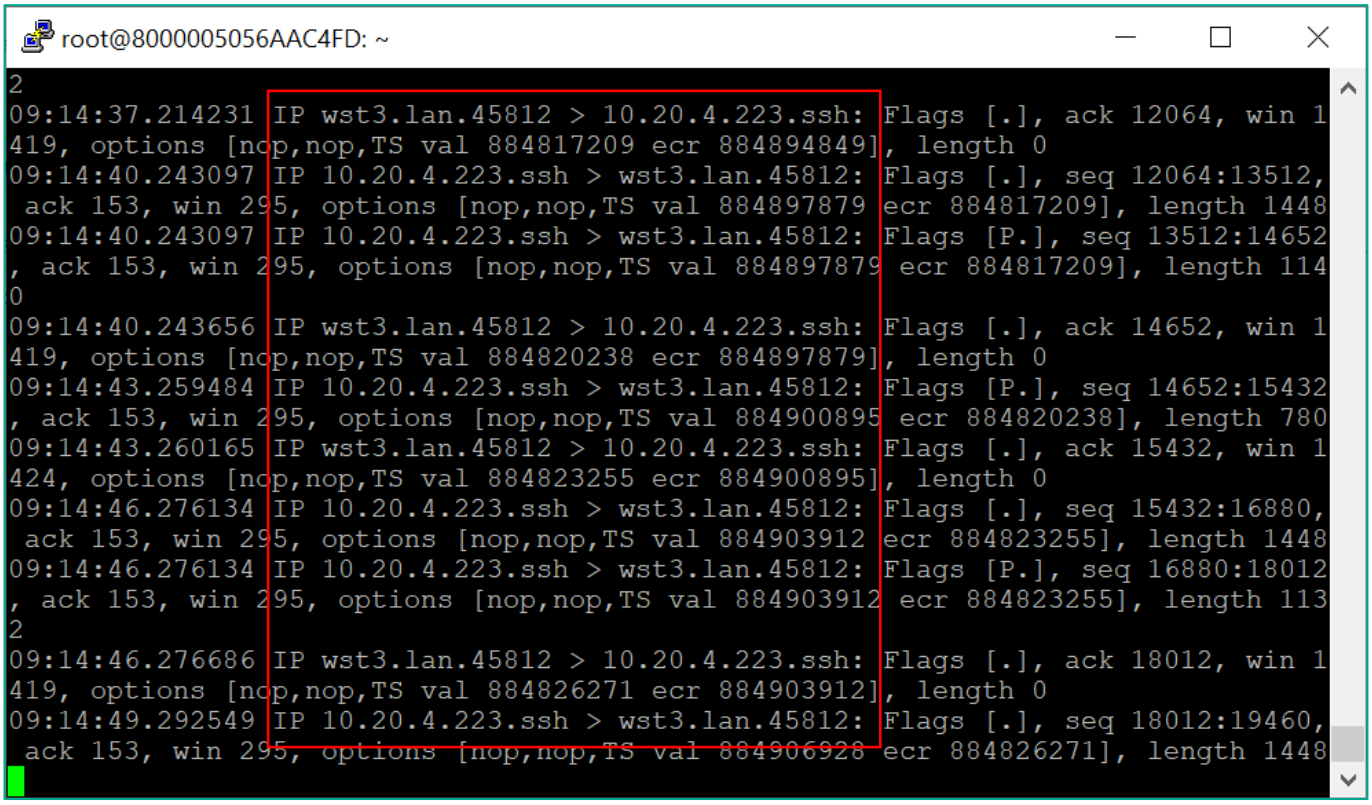
Подключиться к vCPE-3 по SSH и проверить, что трафик переключился на другой WAN интерфейс (в зависимости от настроек, сделанных ранее).

В пункте 3.7.2 проверялось, что трафик идёт через туннельный 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 SSH трафик переключился с интерфейса **genev_sys_4800** (sdwan0) на **genev_sys_4801** (sdwan1).

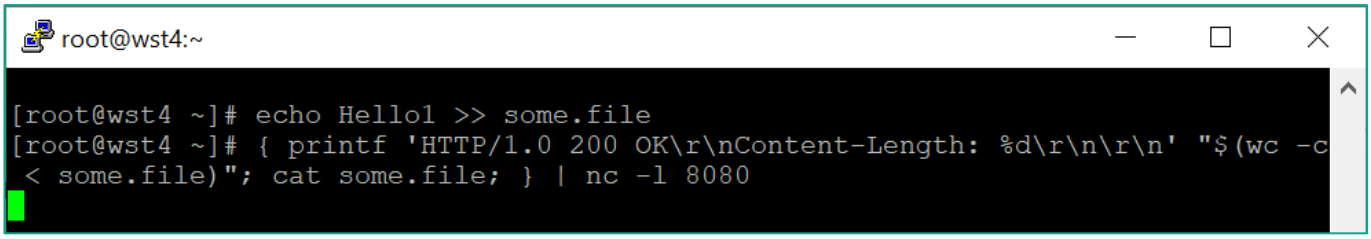


Note: В данном сценарии весь SSH и HTTP трафик с wst3 и wst4 будет перенаправлен в отдельный сервис, куда добавлены только сервисные интерфейсы vCPE3 и vCPE4. Таким образом, с wst3 и wst4 по SSH и HTTP будут доступны адреса только с vCPE3 и vCPE4.

3.7.12. Проверить работу приоритезации HTTP трафика в отдельный транспортный сервис.

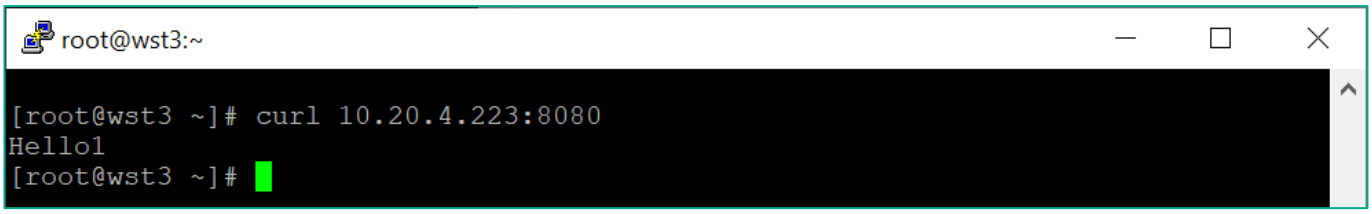
Для генерации тестового трафика HTTP возможно использовать **nc** на **wst4**:

```
echo Hello1 >> some.file

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

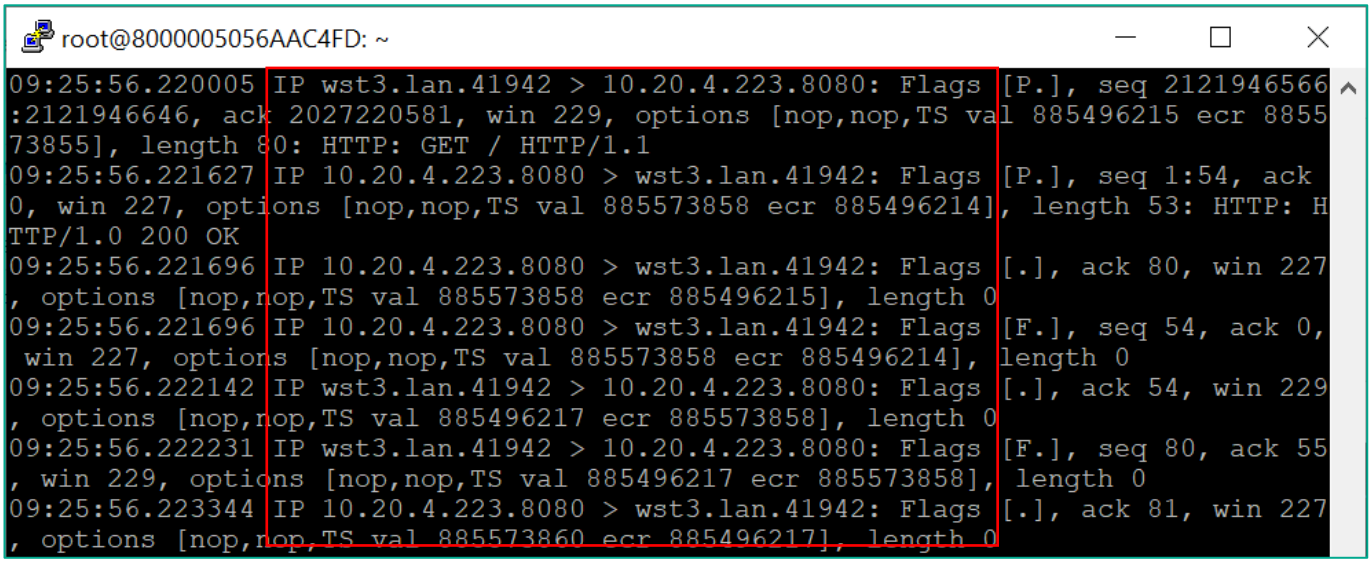


Для генерации HTTP запроса открыть с **wst3** HTTP сессию на порт **8080 wst4**. Например, с помощью **curl**:

```
curl <wst4 IP address>:8080
```



На скриншоте видно, что HTTP трафик переключился с интерфейса **genev_sys_4800** (sdwan0) на **genev_sys_4801** (sdwan1) и DPI распознал HTTP трафик на нестандартном порту.



3.7.13. Вернуть настройки после завершения теста.

Удалить сервис, созданный в п. 3.7.10 (при удалении отметить **Delete associated service interfaces**).

Убрать параметр **Last resort** с линков, добавленный в п. 3.7.3.

Остановить **SSH** сессию от **wst3** до **wst4**, запущенную в п. 3.7.1.

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 CPE не назначено топологических тегов. Такие устройства не устанавливают прямые линки 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 линки между собой.
- Partial-Mesh. Возможно, группировать устройства CPE путем назначения одного топологического тега одной группе устройств и другого топологического тега другой группе. В этом случае все устройства CPE из одной группы (с одинаковым топологическим тегом) пытаются установить прямые линки между собой, а с устройствами из другой группы взаимодействуют через шлюз.

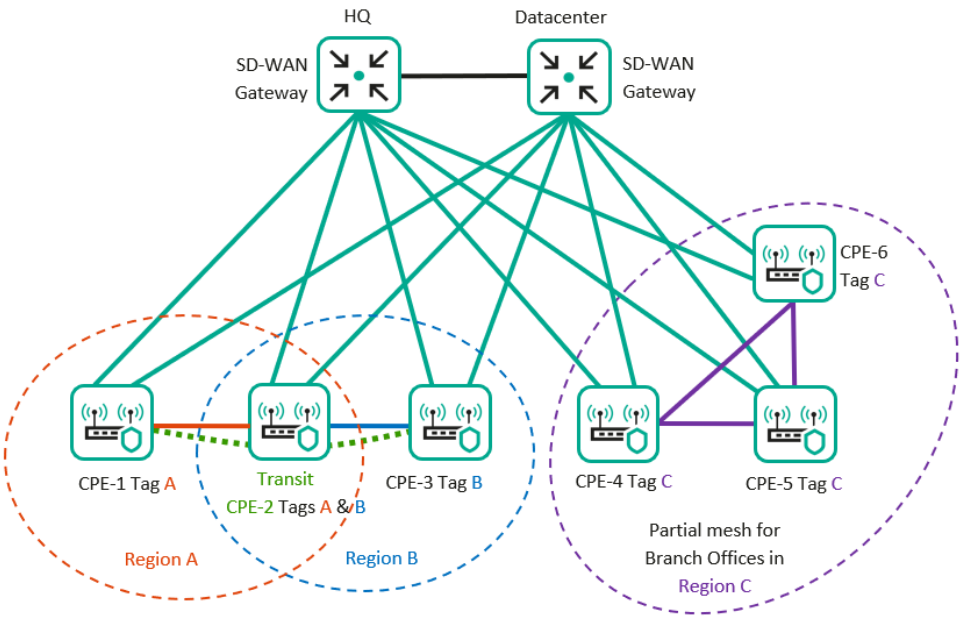


Рис. 4.1 Варианты топологий SD-WAN сети.

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

Также устройство CPE может быть транзитным. В этом случае другие устройства CPE могут устанавливать через него линки.

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

https://support.kaspersky.com/help/SD-WAN/2.3/ru-RU/250984.htm

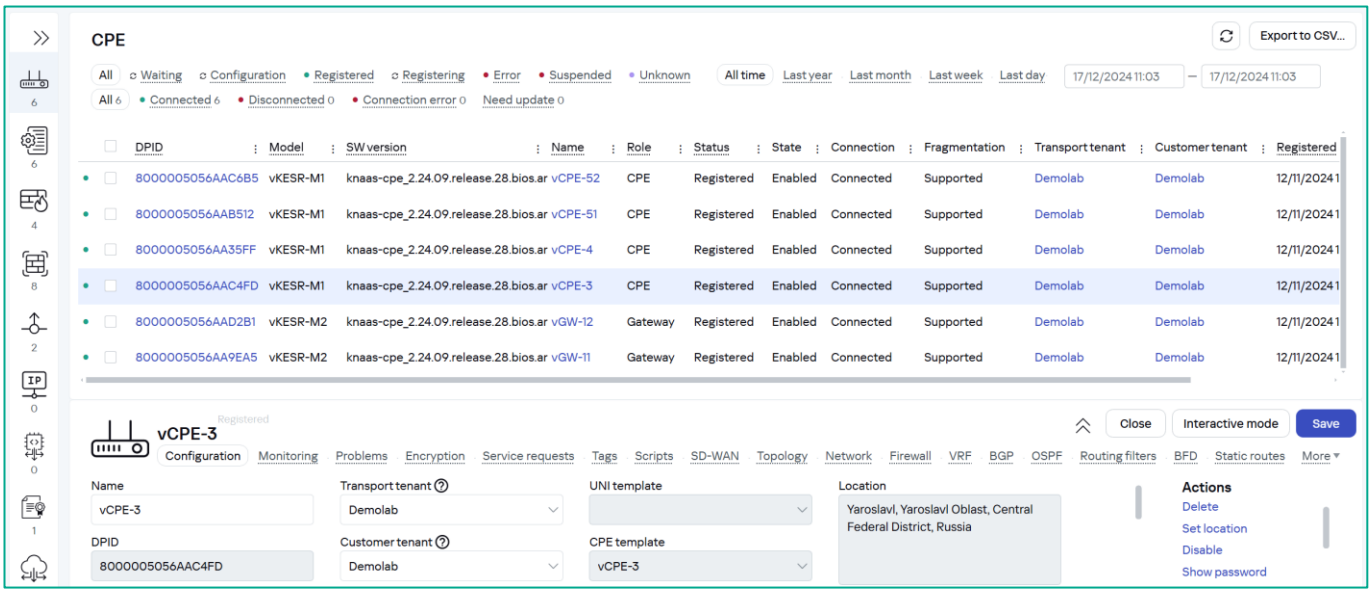
4.1. **Создание топологий Full-Mesh**

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

4.1.1. Задать топологические теги для устройств CPE.

Для создания топологии Full-Mesh устройства CPE должны иметь одинаковые топологические теги.

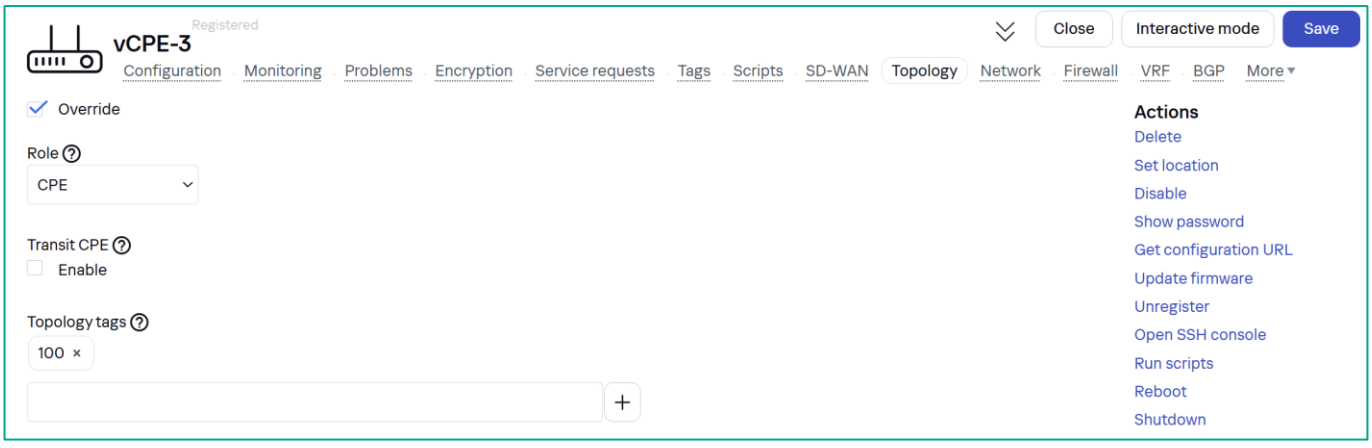
Перейти в меню **CPE** и выбрать **vCPE-3**.



Перейти на вкладку **Topology**

Задать параметры топологии:

- Отметить **Override**
- Добавить тег **100** (нажать на **+)**

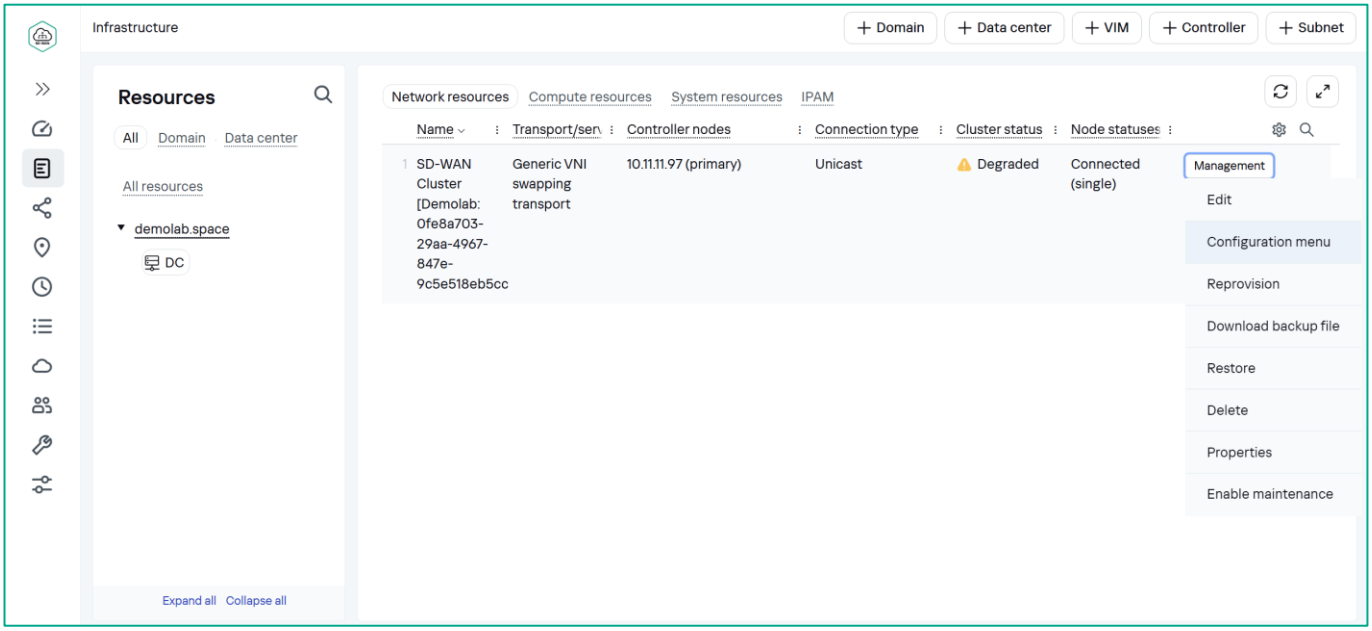


Нажать **Save** (оркестратор применит измененные настройки к CPE).

Назначить топологический тег **100** для устройств **vCPE-4**, **vCPE-51** и **vCPE-52**.

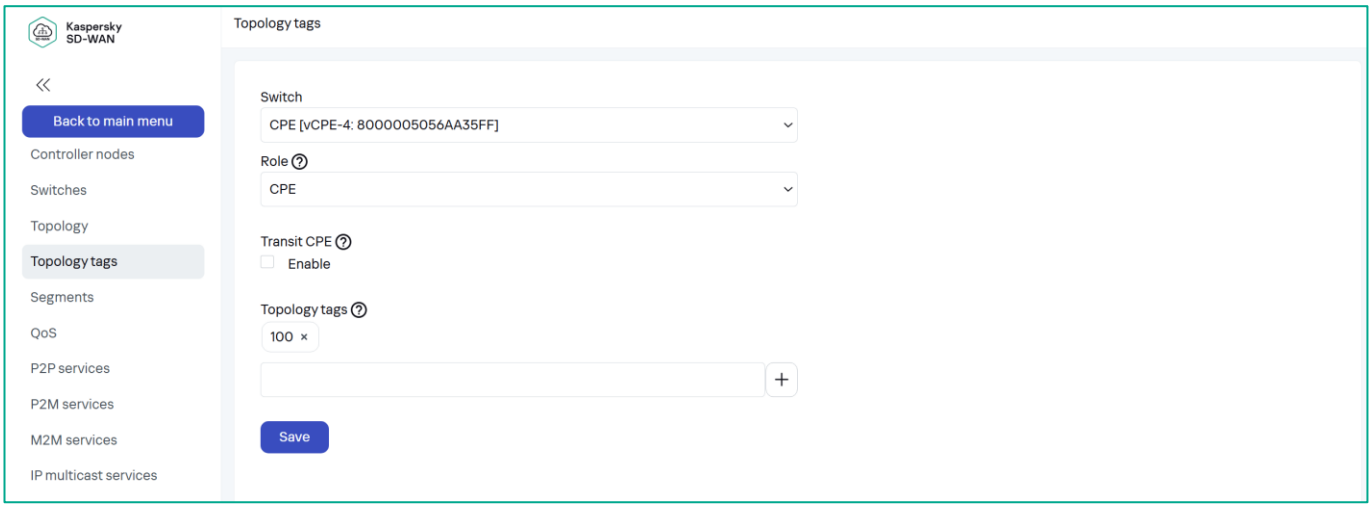
Также возможно назначать топологические теги в настройках контроллера.

Перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu**



Отрыть меню **Topology tags**

Выбрать необходимое CPE и добавить тег (нажать на **+**), затем нажать **Save** для применения настроек.

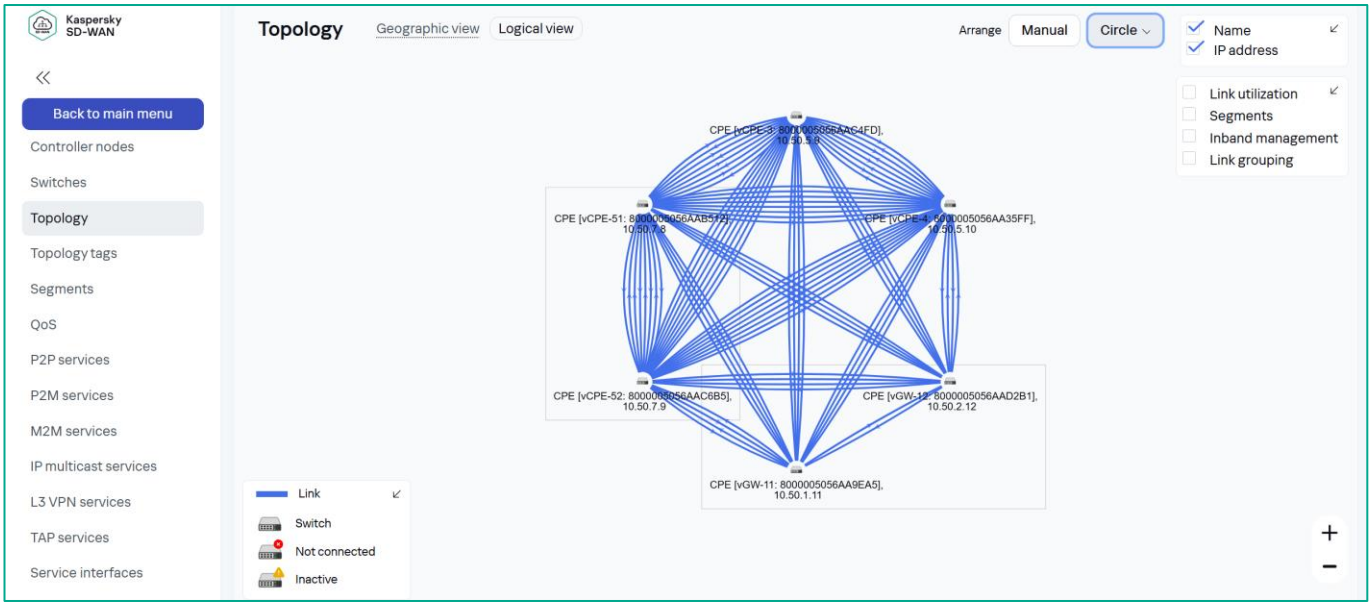


4.1.2. Отобразить построенную топологию.

Для просмотра построенной топологии перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu → Topology**

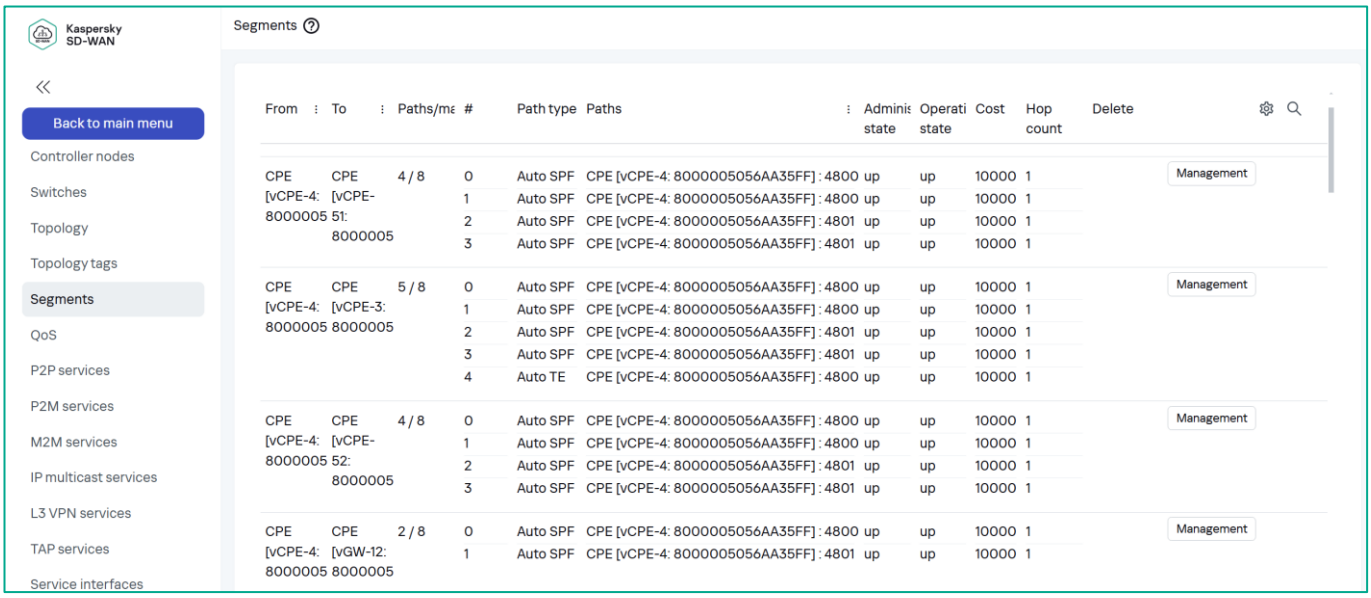
Открыть вкладку **Logical view**. Для удобства отображения выбрать **Arrange**: **Circle**

Отобразится построенная топология сервиса. На скриншоте представлена Full-Mesh топология между CPE, также устройства CPE сохранили линки до vGW-11/12(шлюзов).



Для проверки построенных путей между устройствами CPE перейти на вкладку **Segments**.

Представлен список сегментов, где видны построенные сегменты. На скриншоте ниже видно, что построены сегменты между устройствами CPE, не проходящие через шлюзы(vGW-11/12).



4.1.3. Вернуть настройки после завершения теста.

Убрать топологические теги с устройств CPE, добавленные в п. 4.1.1.

4.2. **Создание топологий Partial-Mesh**

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

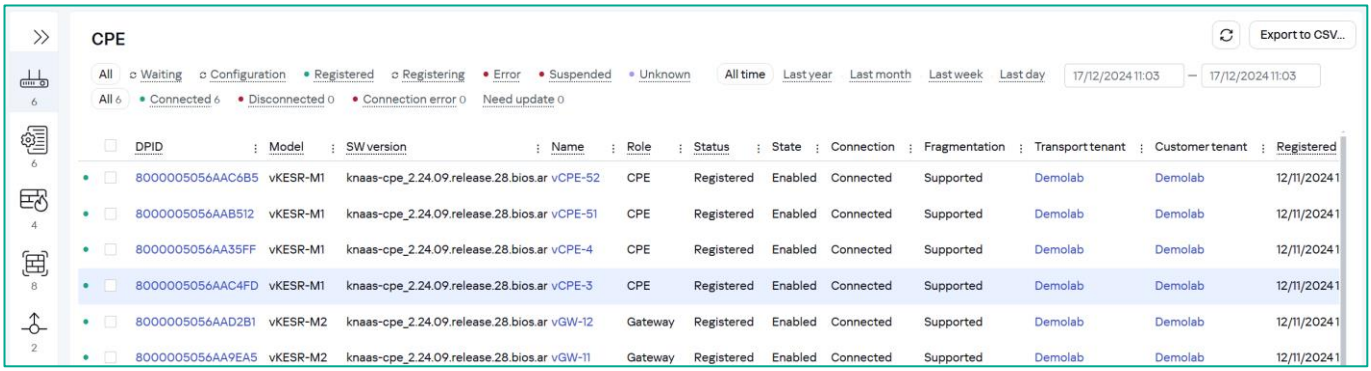
- vCPE-3 и vCPE-4
- vCPE-51, vCPE-52 и vCPE-4

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

4.2.1. Задать топологические теги для устройств CPE.

Для создания топологии Partial-Mesh необходимо задать топологические теги устройствам CPE в соответствии с целевой топологией.

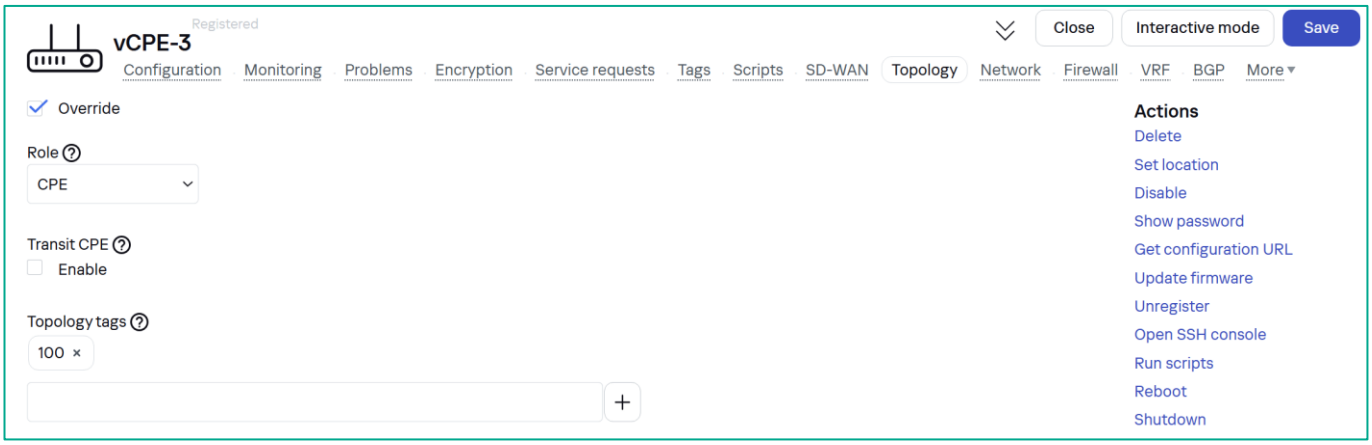
Перейти в меню **CPE** и выбрать **vCPE-3**.



Перейти на вкладку **Topology**

Задать параметры топологии:

- Отметить **Override**
- Добавить тег **100** (нажать на **+)**



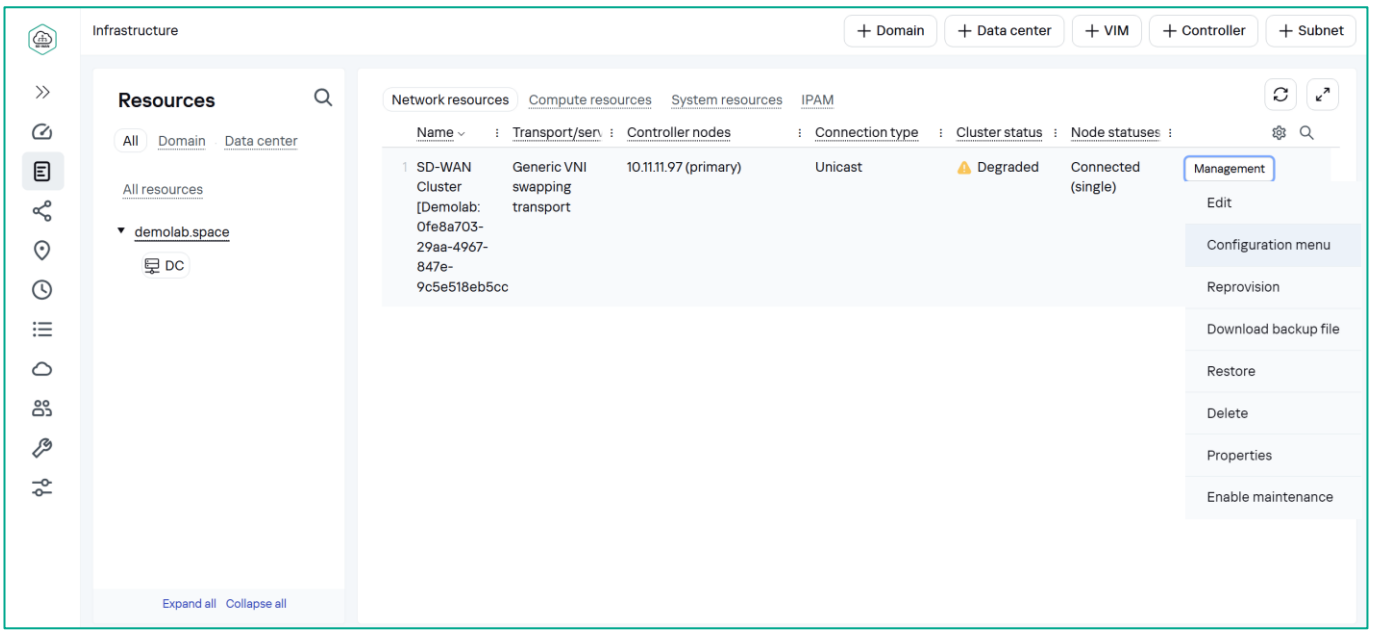
Нажать **Save** (оркестратор применит измененные настройки к CPE).

Назначить топологические теги для остальных устройств CPE:

- **vCPE-51: 200**
- **vCPE-52: 200**
- **vCPE-4: 100** и **200**

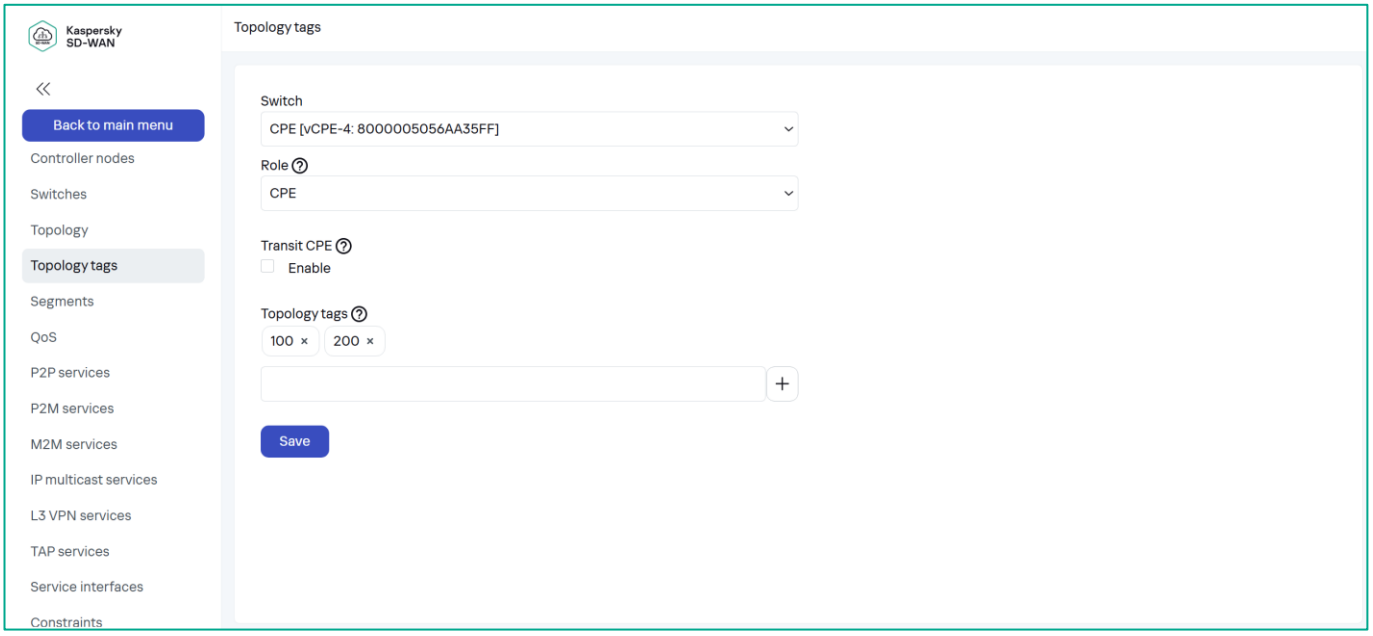
Также возможно назначать топологические теги в настройках контроллера.

Перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu**



Отрыть меню **Topology tags**

Выбрать необходимое CPE и добавить тег (нажать на **+**), затем нажать **Save** для применения настроек.

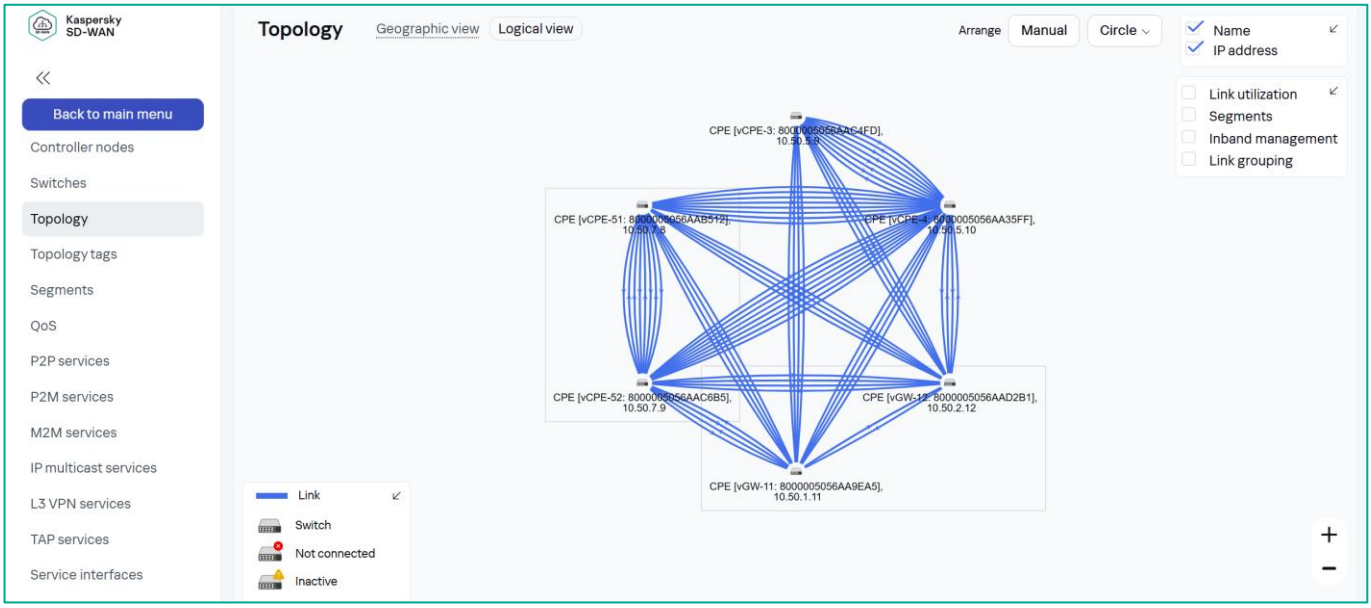


4.2.2. Отобразить построенную топологию.

Для просмотра построенной топологии перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu → Topology**

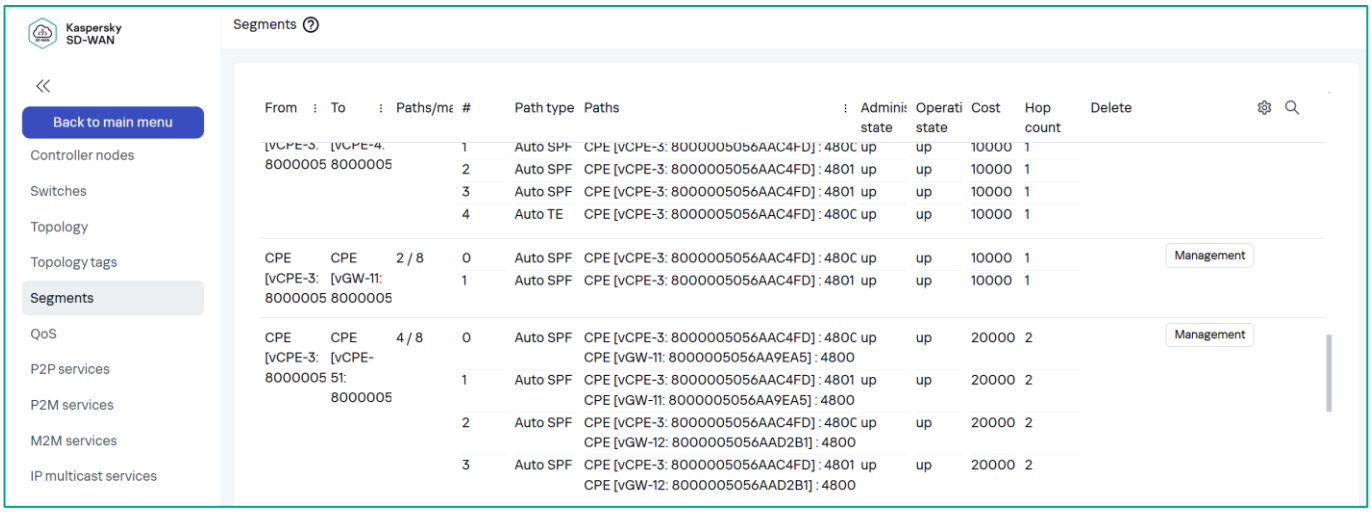
Открыть вкладку **Logical view**. Для удобства отображения выбрать **Arrange**: **Circle**

Отобразится построенная топология сервиса. На скриншоте отображено, что устройства CPE построили линки между CPE-3 и CPE-4, Full-Mesh между CPE-4, CPE-51 и CPE-52, а также сохранили линки до vGW. (шлюзов).



Для проверки построенных путей между устройствами CPE перейти на вкладку **Segments**.

Представлен список сегментов, где видны построенные сегменты. Сегменты образуют Partial-Mesh топологию в соответствии с настроенными тегами (построены прямые линки между vCPE-4 и vCPE-51/52, но не между vCPE-3 и vCPE-51/52).



4.2.3. Вернуть настройки после завершения теста.

Убрать топологические теги и роли с устройств CPE, добавленные в п. 4.2.1.

4.3. **Создание топологий с использованием транзитных CPE**

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

Будут сформированы 2 группы устройств CPE:

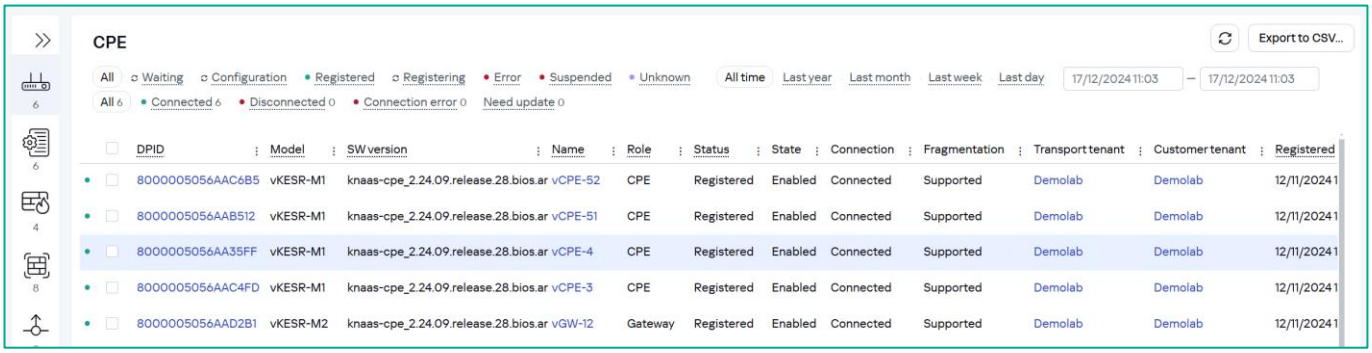
- vCPE-3 и vCPE-4.
- vCPE-4, vCPE-51, vCPE-52.

Каждой группе устройств CPE, будут назначены собственные топологические теги. Устройству vCPE-4 будет назначена транзитная роль, что позволит другим CPE строить линки через данное устройство.

4.3.1. Задать топологические теги для устройств CPE.

Для создания топологии Partial-Mesh необходимо задать топологические теги устройствам CPE в соответствии с целевой топологией.

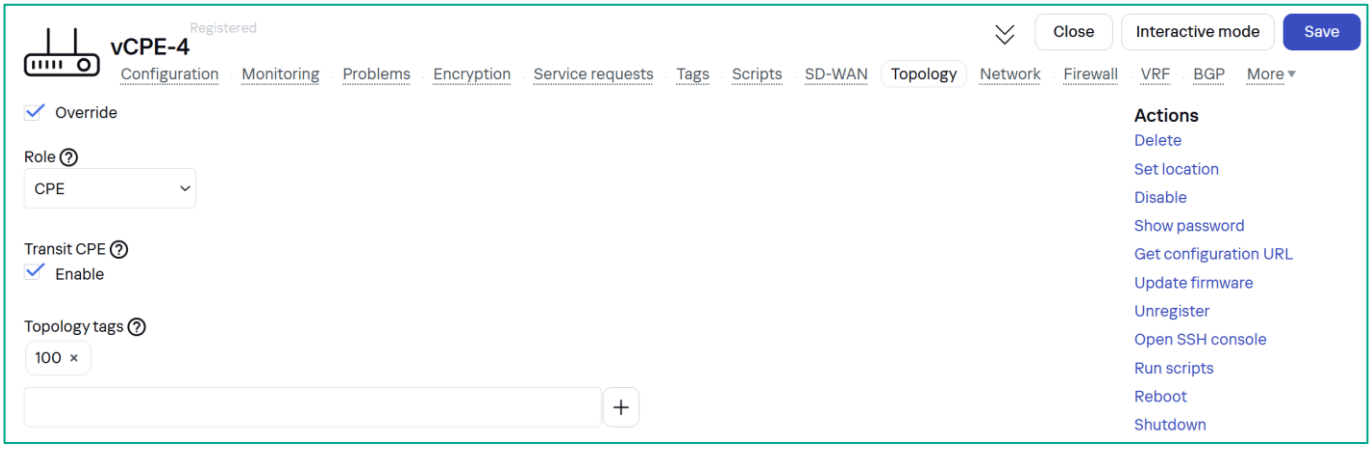
Перейти в меню **CPE** и выбрать **vCPE-4**.



Перейти на вкладку **Topology**

Задать параметры топологии:

- Отметить **Override**
- Отметить **Transit CPE**
- Добавить тег **100** (нажать на **+)**



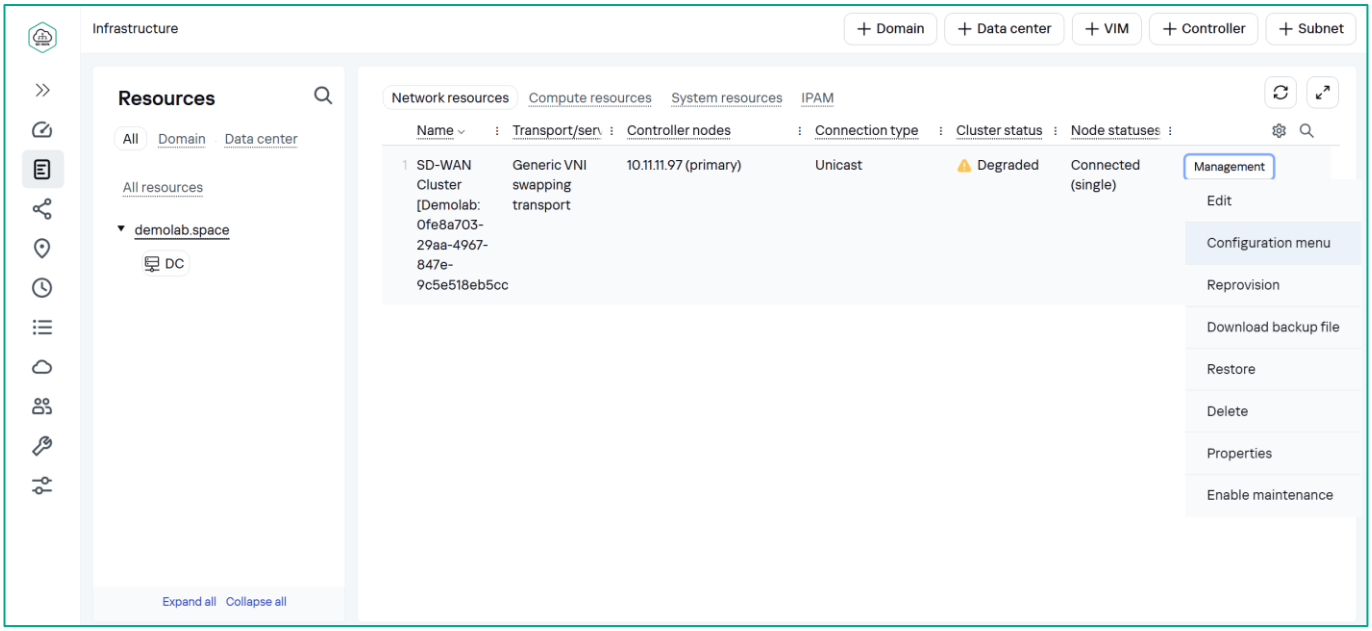
Нажать **Save** (оркестратор применит измененные настройки к CPE).

Назначить топологические теги для остальных устройств CPE (эти CPE не будут транзитными для них не требуется отмечать Transit CPE):

- **vCPE-51: 200**
- **vCPE-52: 200**
- **vCPE-4: 100 и 200**

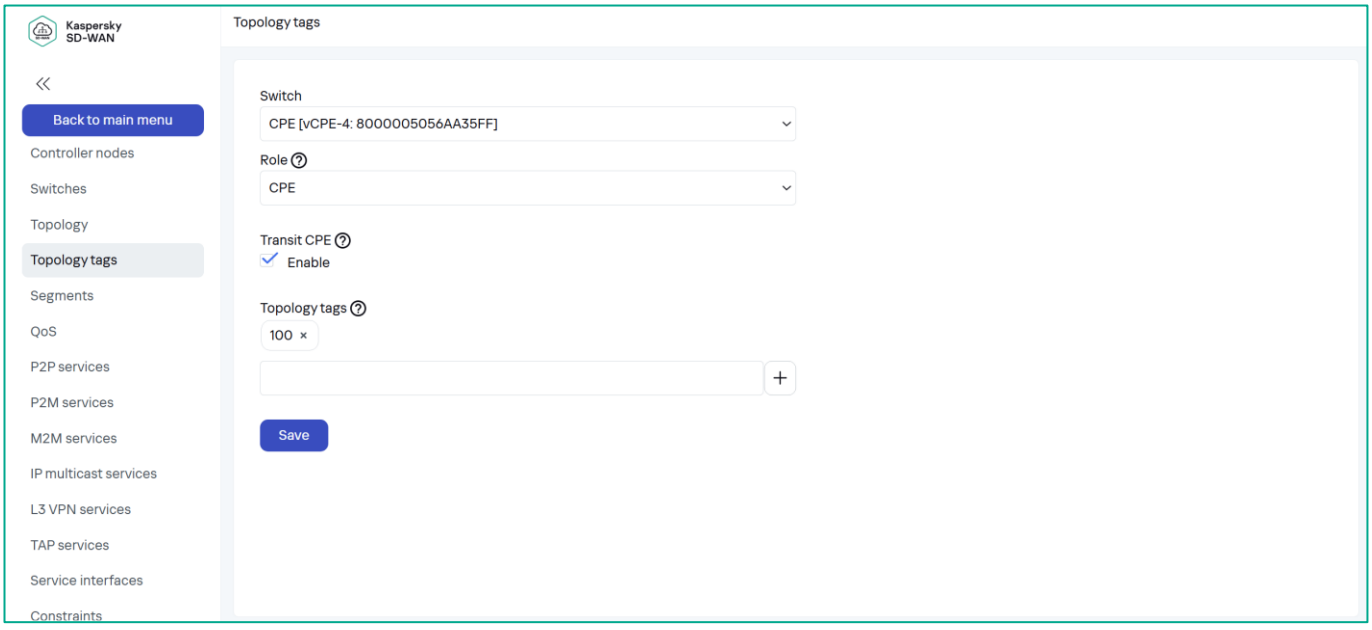
Также возможно назначать топологические теги и роли в настройках контроллера.

Перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu**



Отрыть меню **Topology tags**

Выбрать необходимое CPE, добавить теги (нажать на **+**) и роли, затем нажать **Save** для применения настроек.



4.3.2. Задать максимальное количество автоматических путей SPF.

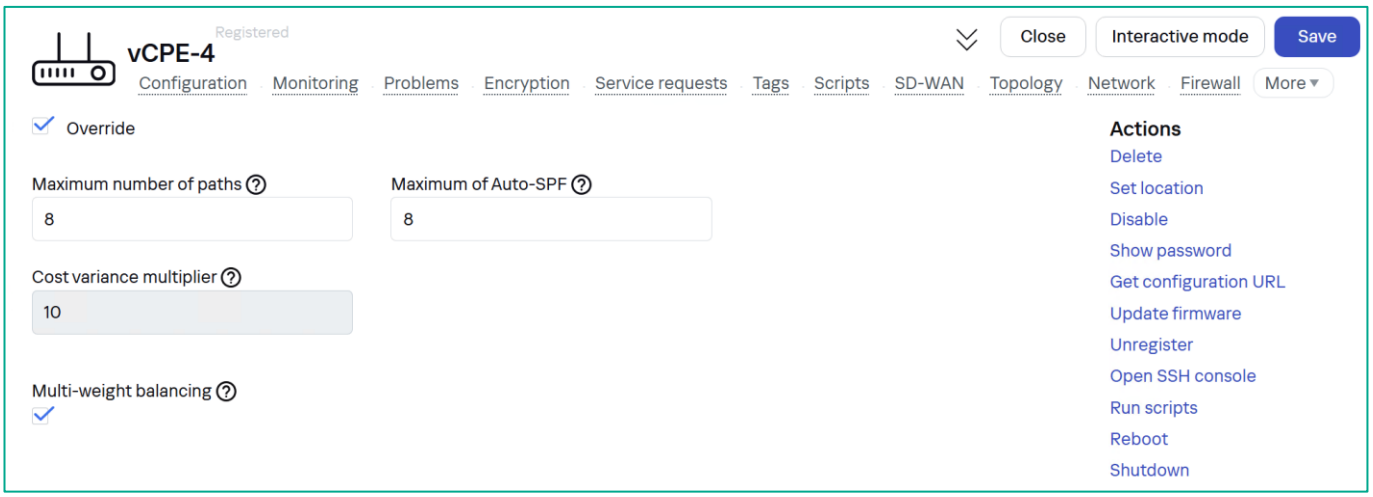
В сценарии требуется увеличить максимальное количество автоматических путей SPF (значение по умолчанию равно 2) для одновременного расчета дополнительных сегментов через транзитное устройство CPE(vCPE-4).

Перейти в меню **CPE** и выбрать **vCPE-4**.

Перейти на вкладку **Multipathing**.

Задать параметры расчёта путей:

- Отметить **Override**
- **Maximum of Auto-SPF: 8**



Нажать **Save**

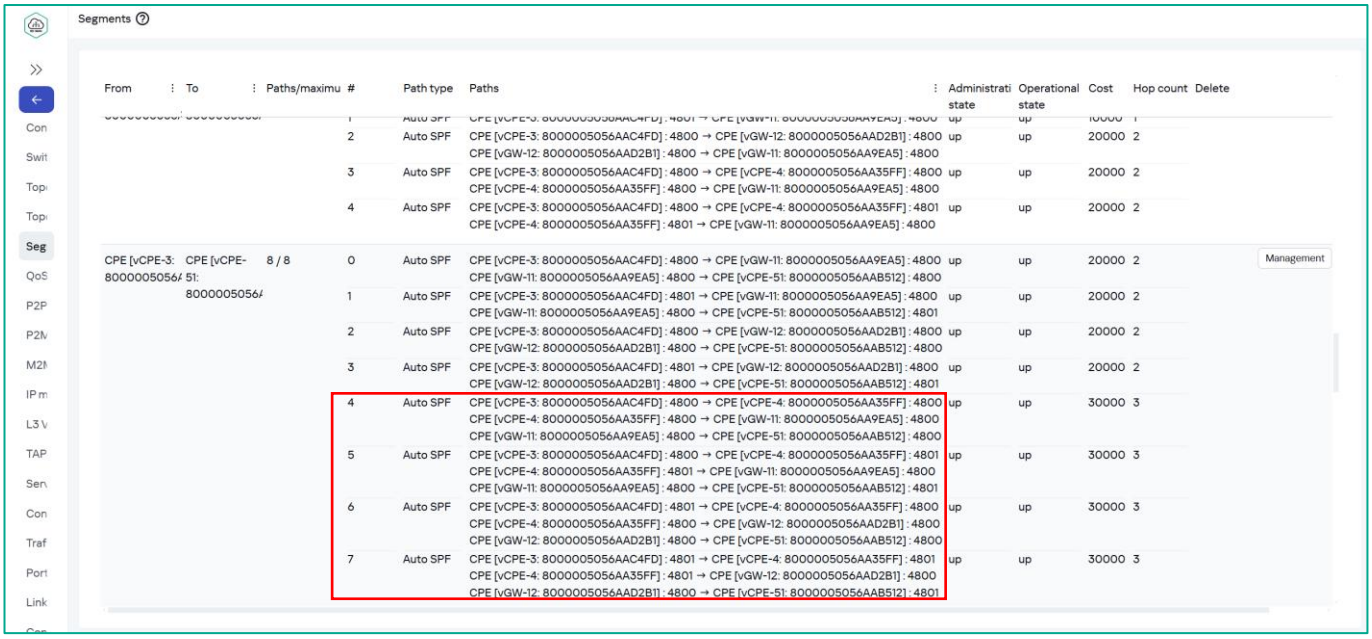
Повторить для **vCPE-3**, **vCPE-51** и **vCPE-52**.

4.3.3. Проверить построенные сегменты через vCPE-4.

Для просмотра построенных сегментов перейти в меню **Infrastructure → SD-WAN контроллер → Configuration menu → Segments**

Отобразится список сегментов, где будут видны построенные пути между устройствами CPE.

На скриншоте представлен сегмент между vCPE-3 и vCPE-51, в рассчитанных путях есть пути через vCPE-4, которому назначена роль Transit CPE.



4.3.4. Вернуть настройки после завершения теста.

Убрать топологические теги и значения Auto-SPF с устройств CPE, добавленные в п. 4.3.1 и 4.3.2.

Приложение A. PoC Checklist

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

N	Название теста	Пункт настройки	Ожидаемый результат	Результат 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 уменьшаются потери пакетов, проходящих через интерфейс, для которого включена эмуляция потерь.	
1.5	Включение мониторинга потерь пакетов на линках.	3.4.2 - 3.4.3	При включении мониторинга потерь в оркестраторе отображается статистика потерь для линков.	
1.6	Включение мониторинга задержек и джиттера на линках.	3.5.2 - 3.5.3	При включении мониторинга задержек и джиттера в оркестраторе отображается статистика задержек и джиттера для линков.	
1.7	Управление трафиком с помощью пороговых ограничений (Constraints).	3.5	При применении ограничений на транспортный сервис из пути прохождения трафика исключаются линки, 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 линки, соответствующих заданным ограничениями.	3.6	Трафик, подпадающий под параметры созданного ACL (protocol UDP, port 5555), перенаправляется в линки, не отмеченные как Last resort.	
1.9	Классификация трафика с помощью DPI и перенаправления в линки, соответствующие заданным ограничениями.	3.7	Трафик, подпадающий под параметры созданного DPI ACL (SSH и HTTP), перенаправляется в линки, не отмеченные как Last resort.	
2	**Построение топологии SD-WAN сети.**			
2.1	Создание топологий Full-Mesh.	4.1	После настройки топологических тегов, устройства CPE создают дополнительные линки для построения Full-Mesh линки (от каждого устройства CPE созданы линки до всех других устройств CPE).	
2.2	Создание топологий Partial-Mesh.	4.2	После настройки топологических тегов, устройства CPE создают дополнительные линки для построения Partial-Mesh топологии. Созданы 2 группы CPE: vCPE-3 и vCPE-4, и vCPE-51, vCPE-52, vCPE-4. CPE данных группы строят прямые линки до всех устройств в своей группе.	
2.3	Создание топологий с использованием транзитных CPE.	4.3	Устройства vCPE-3 и vCPE-51 строят линки через устройство vCPE-4, отмеченное как транзитное.	

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