SC – NEM

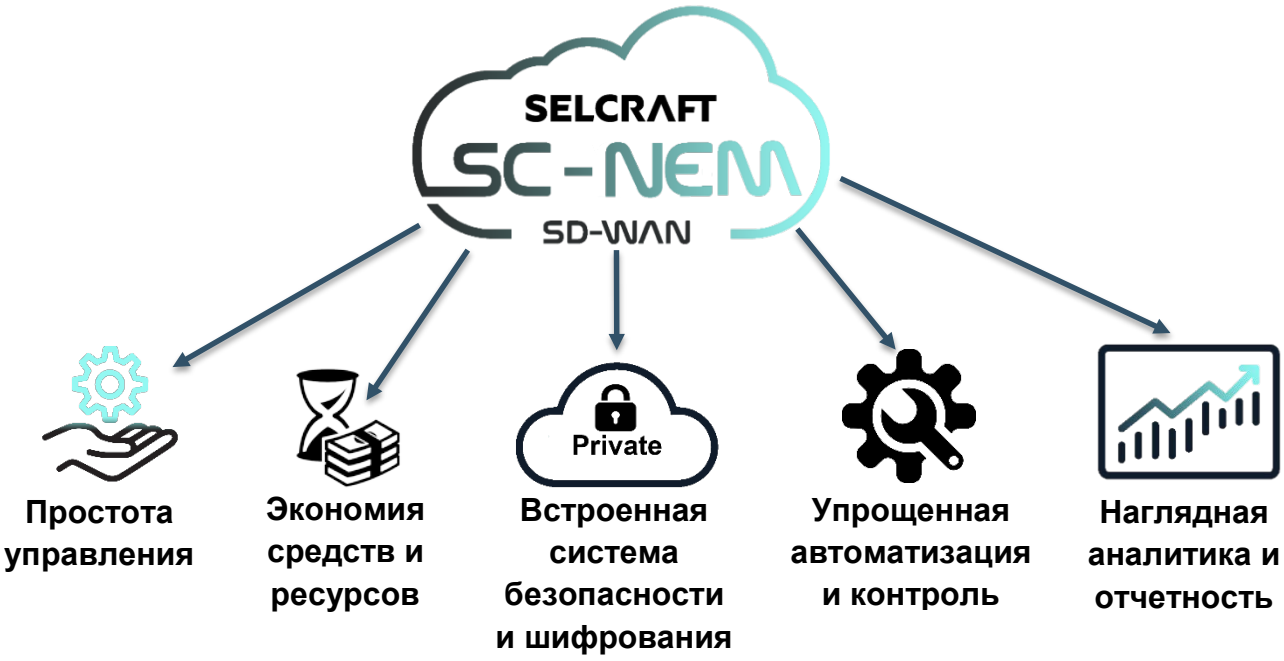
Описание системы

SELCRAFT

Введение

В современных компаниях первостепенными задачами все чаще становятся построение надежной корпоративной сети между филиалами и головным офисом, и развертывание распределенных сервисов. При этом возникает закономерный вопрос: как создать и эксплуатировать такую сеть и сервисы, эффективно управлять ими и избегать серьезных сбоев в их работе?

Selcraft предлагает современное решение, на основе программно-определяемых распределенных сетей (SD-WAN).



1. Что такое SC-NEM

SC-NEM это программное обеспечение для универсальных устройств на базе x86 и ARM (промышленных компьютеров, серверов), которое предоставляет возможность развертывания и последующего управления корпоративной сетью компании, с помощью интуитивно понятного графического интерфейса.

Используя SC-NEM, вы можете безопасно и удаленно управлять сетевой инфраструктурой компании, трафиком отдельных организаций, виртуальными машинами и контейнерами, сервисами, а также осуществлять мониторинг сетей, виртуальных машин и оборудования.

Мы продолжаем модернизировать нашу систему, улучшая возможности функционала и добавляя новый.

С полным списком доступных функций ПО можно ознакомится ниже (Раздел 1.5).

1.1. Из чего состоит SC-NEM

Система SC-NEM состоит из следующий компонентов:

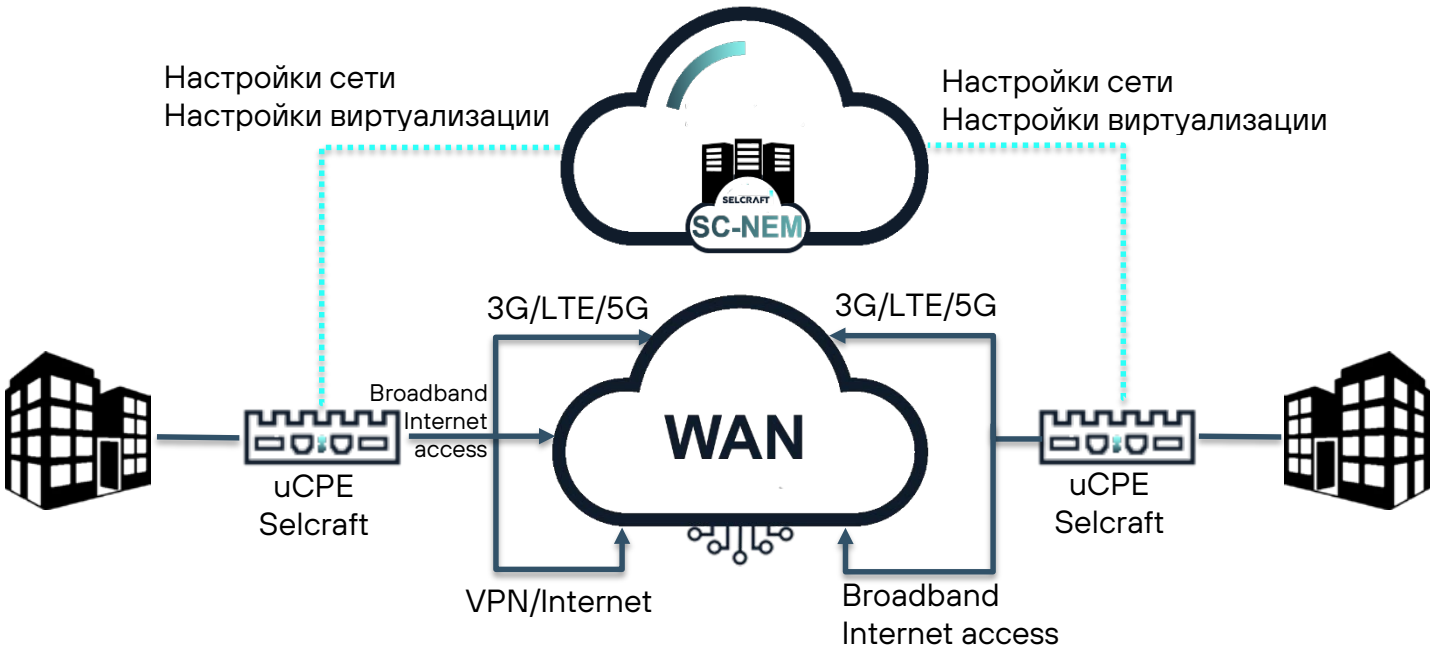
- Внешних пользователей:
  - Пользователи – администраторы и прочий персонал, осуществляющий работу в системе с помощью клиентских рабочих станций.
  - Внешние Системы – сторонние OSS/BSS системы;
- Внешних устройств:
  - Физические устройства – uCPE и подобные устройства, играющие роль Узлов в построении сетевой инфраструктуры;
  - Виртуальные машины – ВМ и контейнеры, развернутые на физических устройствах.
- Внешних служб:
  - NTP – служба синхронизации врмени;
  - DNS – служба доменных имен;
  - SSH – служба удаленного управления системой и тунеллирования TCP-соединений;
- Внутренних компонентов:
  - Контроллер – компонент отвечающий за применение конфигураций к Узлам;
  - WEB сервис – сервис, обеспечивающий работу WEB приложения (сайта);
  - Сервис аутентификации – сервис, выполняющий функции по авторизации внешних пользователей в системе;
  - Сервис мониторинга – сервис, выполняющий функции по предоставлению и хранению данных о работе компонентов системы;
  - Асинхронный сервер – сервис, выполняющий функции по автономному выполнению сформированных задач на компонентах системы;
  - База данных - сервис, выполняющий функции по хранению данных системы и сформированных задач.
  - Прочие компоненты необходимые для реализации дополнительных функций.

Взаимодействие между Внешними пользователями, Внешними службами, Внутренними и Внешними компонентами Системы осуществляется через информационные потоки, посредством протоколов IP.

1.2. Для чего нужна SC-NEM

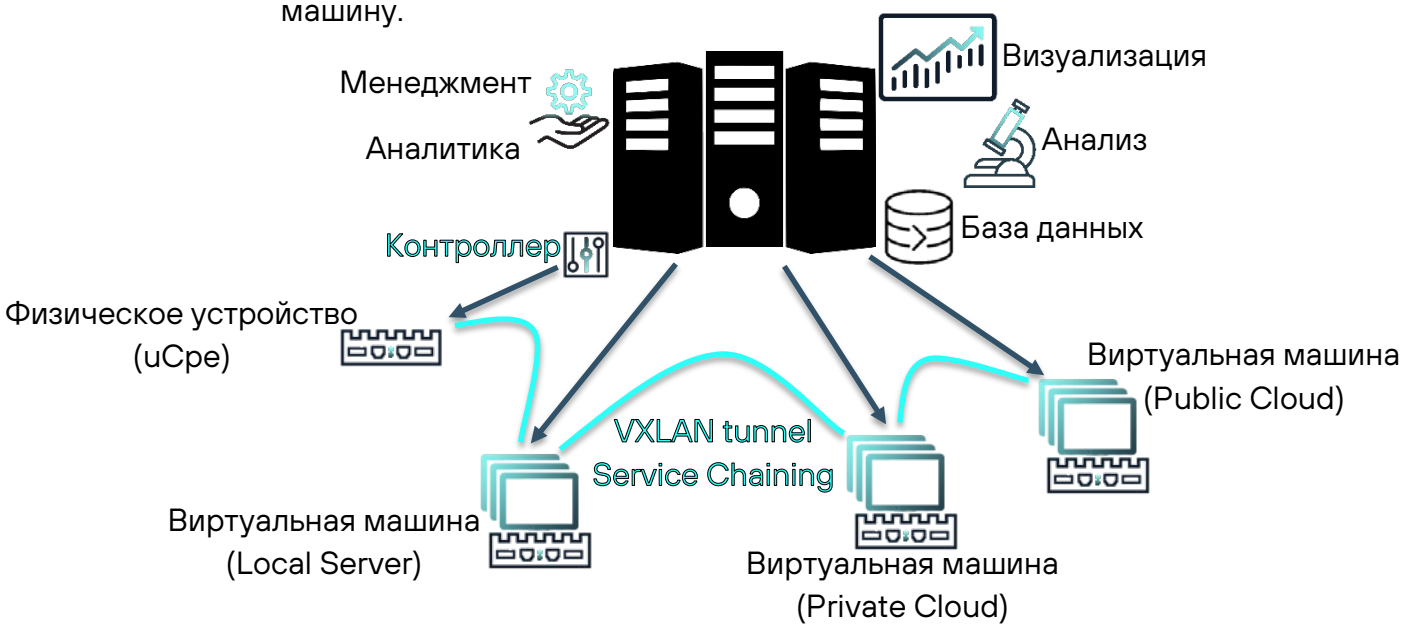
❖ Построение WAN сетей уровня предприятия, автоматизация настроек сети и разворачивания сервисов:

- SC-NEM упрощает внедрение WAN сетей и многоблочных сетей, объединяя политики доступа к облаку региональных филиалов в единый инструмент. Это позволяет сегментировать и надежно изолировать корпоративную инфраструктуру, состоящую из гостевых беспроводных связь, направлений бизнеса, деловых партнеров и многого другого.



❖ Построение гибридной Cloud Native сети

- SC-NEM дает доступ к работе с несколькими облакам (локальным, частным, публичным), для обеспечение связности и построение WAN сети в соответствии с корпоративными правилами. Возможно установить программное обеспечение как на физическую uCPE так и на виртуальную машину.



1.3. Полный перечень функционала SC-NEM

На данный момент SC-NEM предоставляет следующий набор функциональности:

❖ Управление Организациями	• Добавление Организаций; • Редактирование атрибутов Организаций; • Привязка Узлов к Организации; • Просмотр списка существующих шаблонов конфигурации Узлов и их параметров; • Управление локальными и публичными образами; • Управление топологиями L2 VPN и L3 VPN Организации; • Просмотр истории применения топологий • Настройка параметров IP; • Добавление логических маршрутизаторов; • Управление IP диапазонами логических маршрутизаторов; • Управление листами доступа (ACL); • Настройка параметров лицензирования; • Настройка параметров безопасности; • Настройка параметров хранилища данных мониторинга и журналов событий; • Просмотр истории применения Системных настроек (лицензирование, безопасность, хранилище) • Настройка параметров мониторинга; • Просмотр истории применения настроек мониторинга; • Просмотр сообщений о работе Узлов Организации; • Просмотр статистики о работе Узлов Организации.

❖ Управление Группами	• Добавление Групп; • Редактирование атрибутов Групп; • Привязка узлов к Группе; • Управление топологиями L2 и L3 VPN Группы; • Просмотр истории применения топологий; • Просмотр сообщений о работе Узлов Группы; • Просмотр статистики о работе Узлов Группы.
❖ Управление Узлами	• Редактирование атрибутов Узла; • Перемещение Узла в Организации/между Группами; • Добавление (создание) Виртуальных машин/Контейнеров на Узле; • Удаление Виртуальных машин/Контейнеров; • Просмотр статистики о работе Виртуальных машин/Контейнеров Узла; • Применение текущей конфигурации Узла к Системе; • Просмотр текущей конфигураций Узла; • Просмотр примененных и ранних конфигураций Узла; • Сравнение текущей и примененной конфигураций Узла; • Отмена изменений текущей конфигурации Узла; • Создание шаблона из текущей конфигурации Узла; • Восстановление текущей конфигурации Узла из ранних конфигураций; • Просмотр истории примененных конфигураций • Просмотр сообщений о работе Узла; • Просмотр статистики о работе Узла.

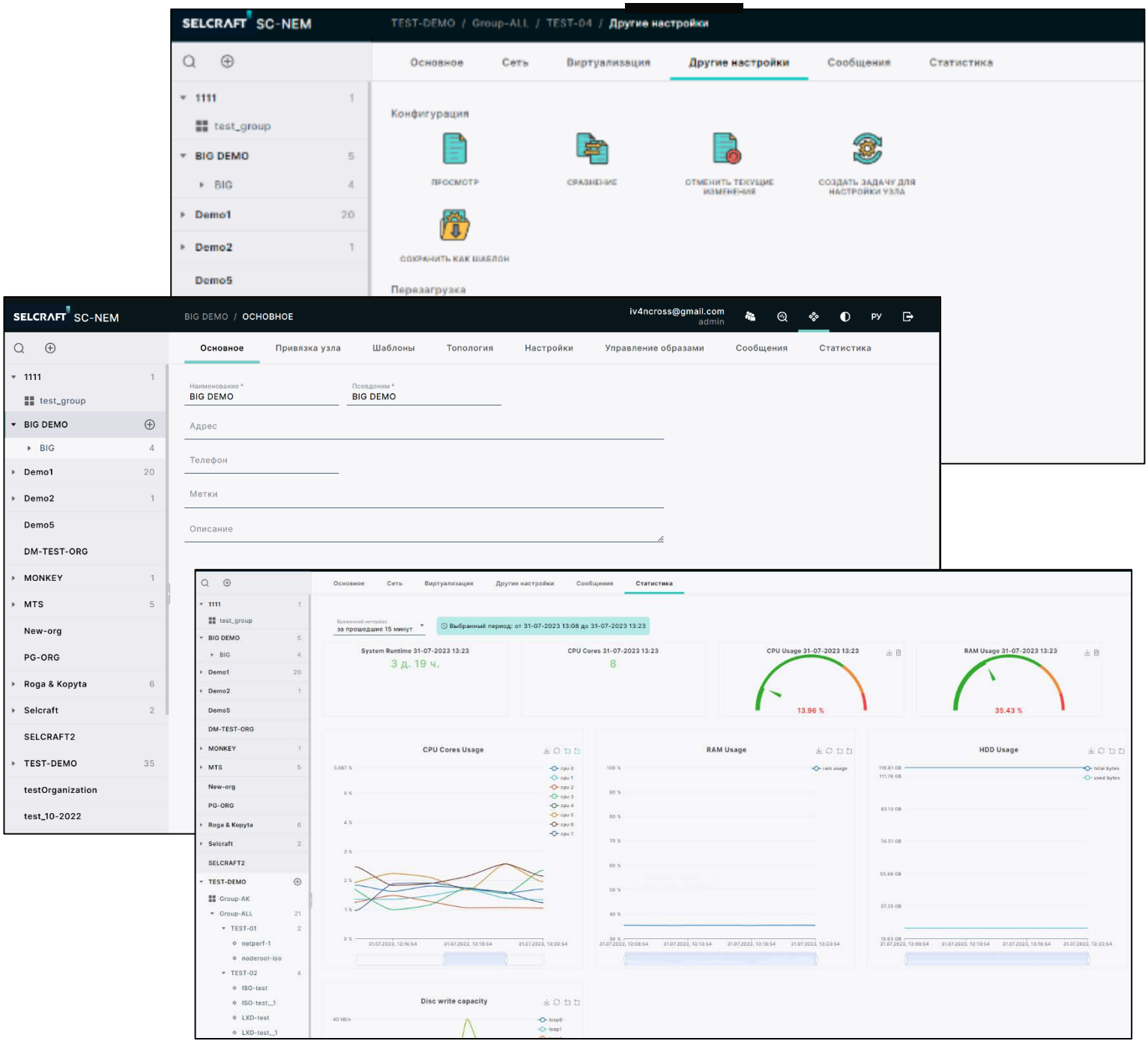
❖ Управление сетевыми настройками Узла	• Создание, редактирование и удаление сетей; • Настройка DHCP; • Настройка VRRP; • Управление WAN подключениями; • Настройка конфигурации конечных точек доступа WiFi; • Настройка конфигурации NAT; • Настройка конфигурации Routing; • Настройка конфигурации правил Rate-Limit, Route-Map, SPAN, QoS; • Просмотр статистики о работе сетевых интерфейсов Узла.
❖ Управление Виртуальными машинами и Контейнерами	• Редактирование атрибутов ВМ/Контейнеров; • Запуск и остановка ВМ/Контейнеров; • Доступ к консоли ВМ/Контейнера; • Создание снимков ВМ/Контейнеров; • Создание образов из снимков ВМ/Контейнеров; • Восстановление ВМ/Контейнеров из снимков; • Просмотр сообщений о работе ВМ/Контейнера; • Просмотр статистики о работе ВМ/Контейнера.
❖ Управление пользователями	• Добавление пользователей; • Редактирование атрибутов пользователей; • Блокировка пользователей; • Просмотр истории удачных и неудачных попыток входа пользователей в Систему; • Сброс/восстановление/смена пароля пользователем.
❖ Дополнительные возможности	• Создание условий для удаленного доступа к локальным сетям Организаций; • Первичная настройка Узла посредством командной строки; • Тестирование пропускной способности сетей с помощью Netpref.

2. Пользовательский интерфейс

Пользовательский интерфейс (GUI) представляет собой совокупность интерактивных и не интерактивных графических элементов, сгруппированных в определённые Функциональные группы, расположенные на отдельных веб-страницах.

Доступ к страницам осуществляется с помощью протокола HTTPS и веб-браузера, что позволяет получить доступ к функциям Системы с любого устройства, имеющего доступ к сети компании.

Дизайн GUI разработан с целью серьезно облегчить и ускорить процесс адаптации Пользователей к работе с Системой SC-NEM.

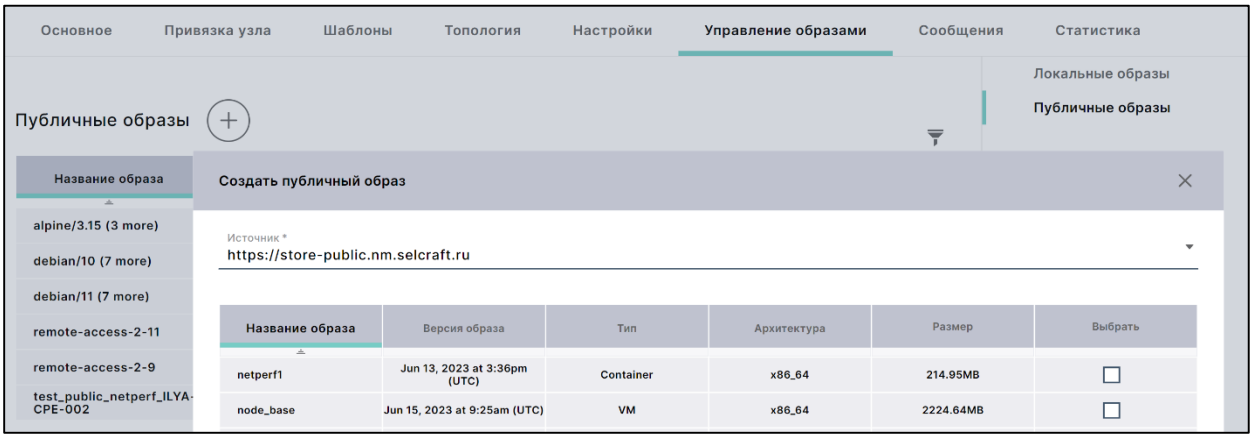


3. Подробное описание некоторых из доступных функций

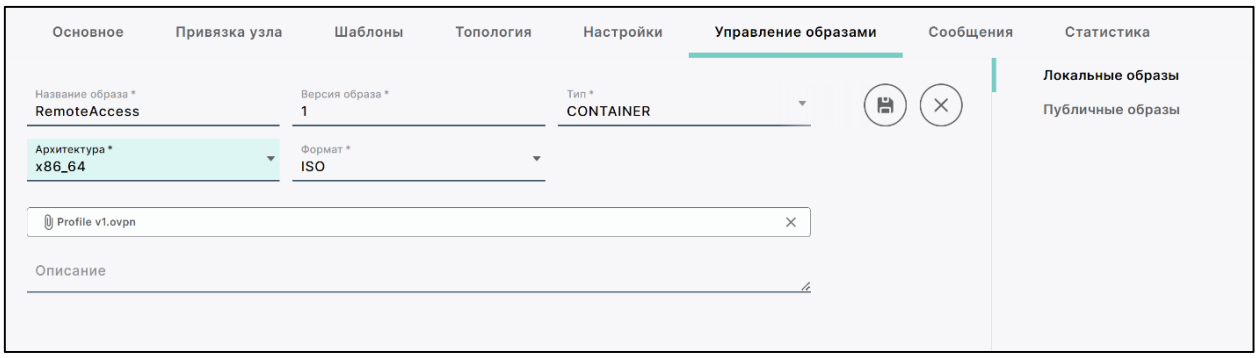
3.1. Управление Организациями – локальные и публичные образы

Функционал системы позволяет использовать образы - сохраненные конфигурации Виртуальных машин и Контейнеров. Для развертывания ВМ/Контейнера с использованием образа, он должен быть добавлен в Организацию.

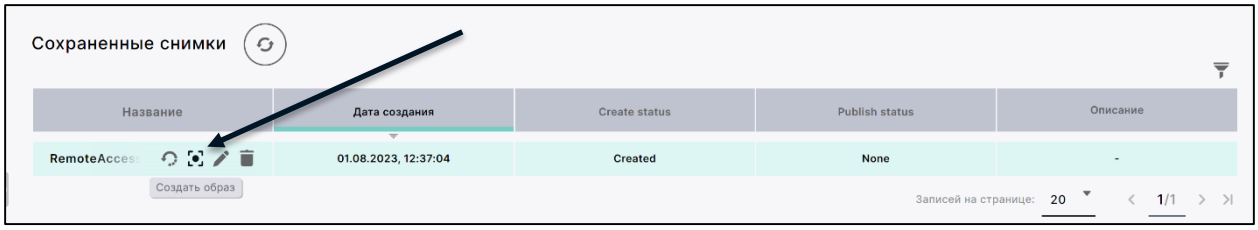
Публичные - добавляются в Организацию из публичных источников, доступных для всех Организаций:



Локальные – добавляются в Организацию вручную, с использованием конфигурационного файла:



Либо создаются из снимков ВМ/Контейнеров, принадлежащих этой Организации:



3.2. Управление Группами – топологии L2 VPN и L3 VPN

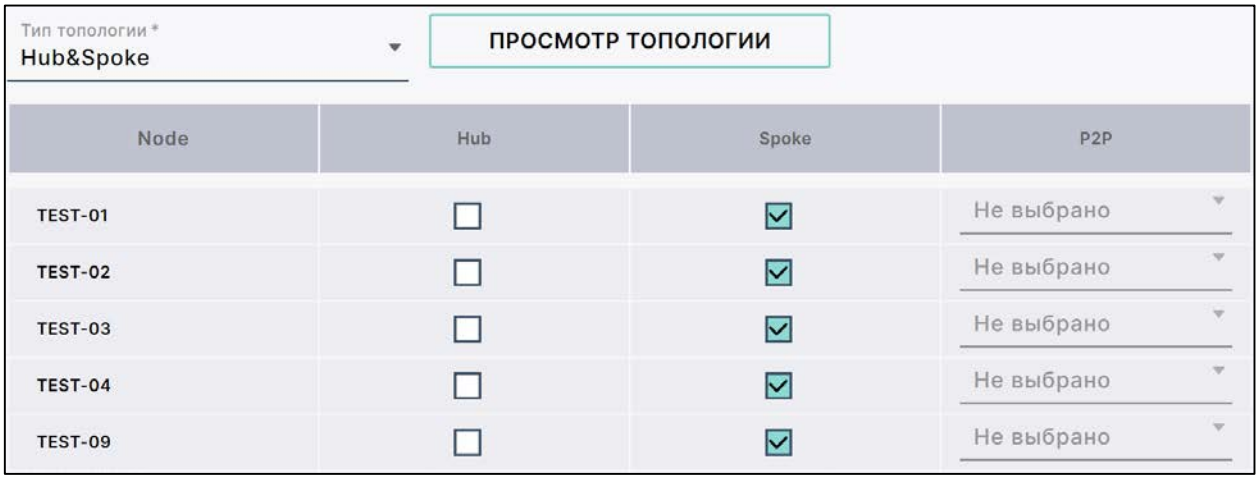
Функционал системы позволяет управлять топологиями виртуальных (VPN) соединений Узлов в Группах (и Организациях) для L2 и L3 уровня соответственно.

L2 топологии основаны на локальных сетях Узлов, L3 – на соединениях логических маршрутизаторов (VRF).

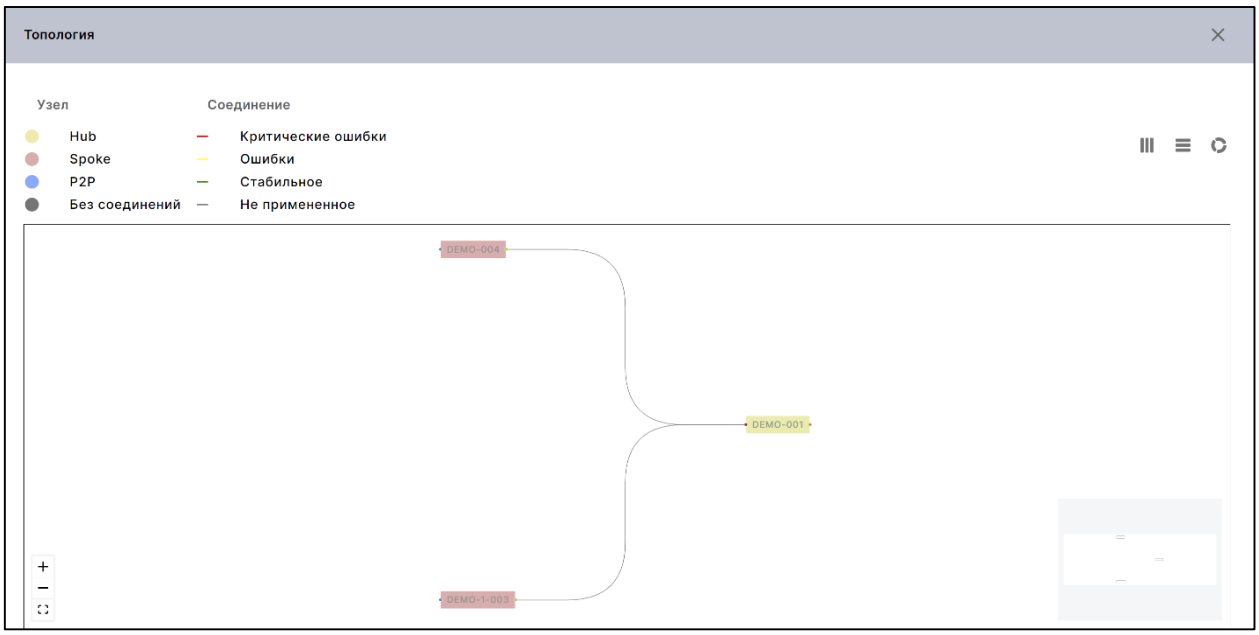
Все топологии могут быть построены согласно трем основным типам Full Mesh (каждый с каждым), Hub&Spoke (звезда) и Ponint-to-Point (точка к точке).

В системе предусмотрена функция выбора типа тоннелей VPN соединений и типа VPN-шифрования.

При добавлении/редактировании пользователь может добавлять/исключать Узлы из топологии, выбирать их тип в топологии, создавать P2P пару для каждого из Узлов:



Также пользователю доступен просмотр созданной топологии в графическом формате:

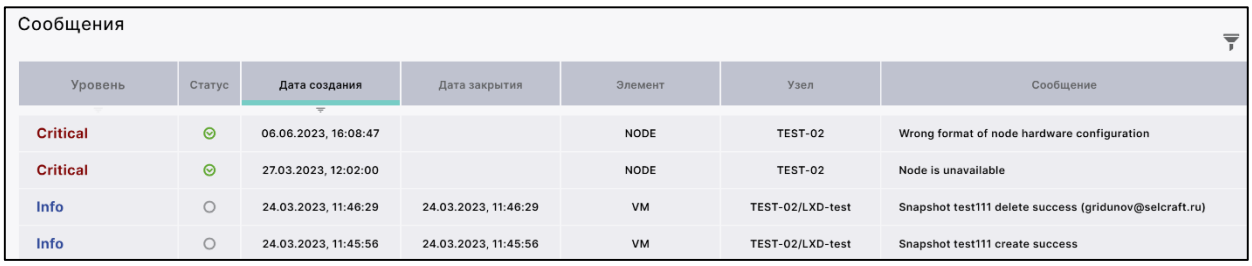


3.3. Управление Узлами - просмотр сообщений и статистики о работе ВМ/Контейнеров

Функционал системы позволяет осуществлять мониторинг работы ВМ/Контейнеров, развернутых на одном Узле. (Аналогичный функционал доступен для мониторинга общей работы Узлов в Организациях/Группах, отдельных компонентов Узлов, и прочих внутренних компонентов системы).

Для этого пользователю доступен просмотр серверных сообщений и статистики в графическом виде.

Серверных сообщения формируются автоматически и содержат сведения о возникших ошибках в ходе работы, а также о статусе применения настроек, и прочую информацию:



Статистика представлена в виде графиков и отражает статусы работы компонентов в реальном времени. Например, процент загруженности процессоров Узла или времени безотказной работы:

При просмотре статистики доступен выбор временного интервала, за который представлены статистика.

3.4. Управление сетевыми настройками Узлов – правила

Системы позволяет осуществлять настройку правил для трафика, проходящего через сеть Узла.

Функционал включает в себя настройку правил:

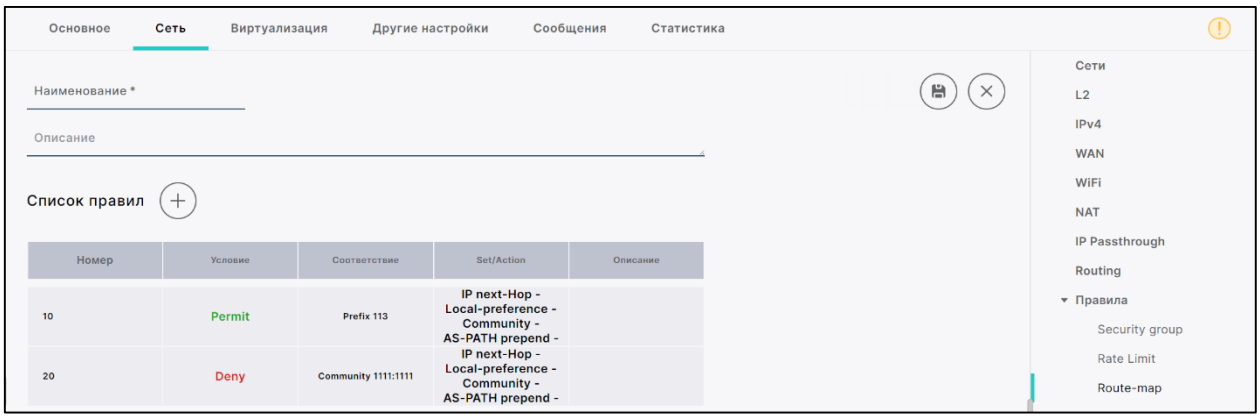
Access Control List (ACL) - листы доступа к управлению, которые определяют, в каких сетях могут быть применены правила передачи пакетов данных:

ACL являются частью параметров Организации и применяются при настройке прочих правил на Узлах.

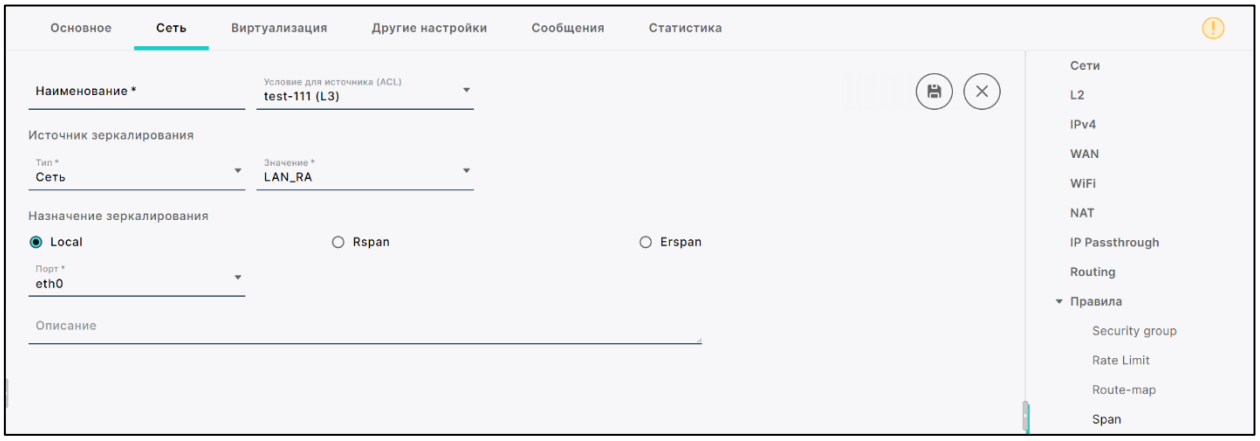
Security group - сеть или группа сетей, к которым применяются ограничения ACL.

Rate Limit – правила ограничения скорости передачи данных между сетями:

Route-map – правила фильтрации маршрутов и применения различных атрибутов для маршрутов:



SPAN/RSPAN/ERSPAN – правила зеркалирования трафика:



Данные правила позволяют настроить маршрутизатор так, чтобы все пакеты, приходящие на один порт или группу портов этого маршрутизатора, дублировались на другом, с целью их дальнейшего анализа и мониторинга:

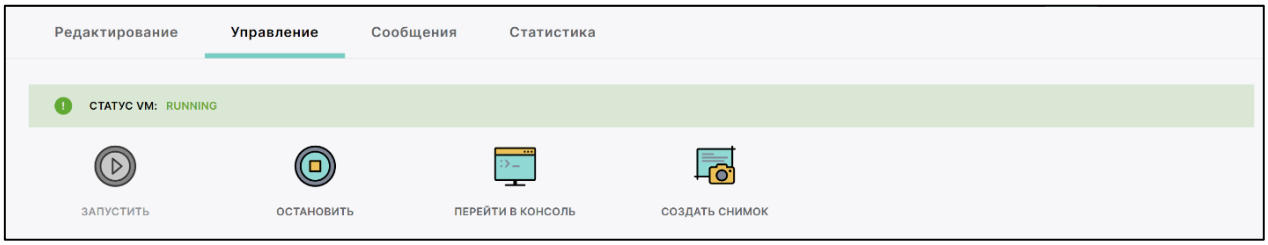
Quality of Service (QoS) – правила предоставления приоритетов обслуживания для различных типов трафика:

Для QoS возможно создавать основные и дочерние полиси. Основная полиси распространяется на весь трафик, проходящий через выбранные порты Узла, дочерние – на части этого трафика.

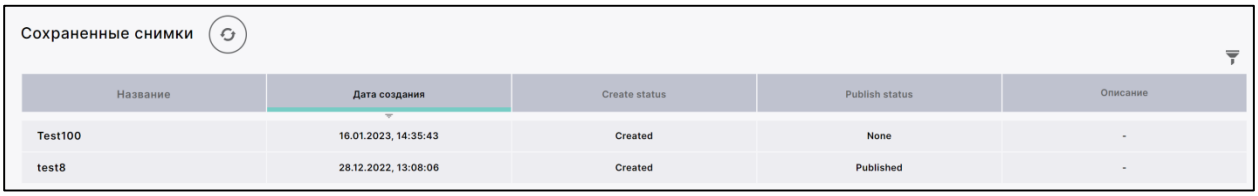
3.5. Управление ВМ/Контейнерами – остановка/запуск, снимки, консоль

Функционал системы позволяет легко управлять развернутыми ВМ и Контейнерами из GUI.

Пользователю доступны остановка и запуск ВМ, открытие консоли, создание снимков:



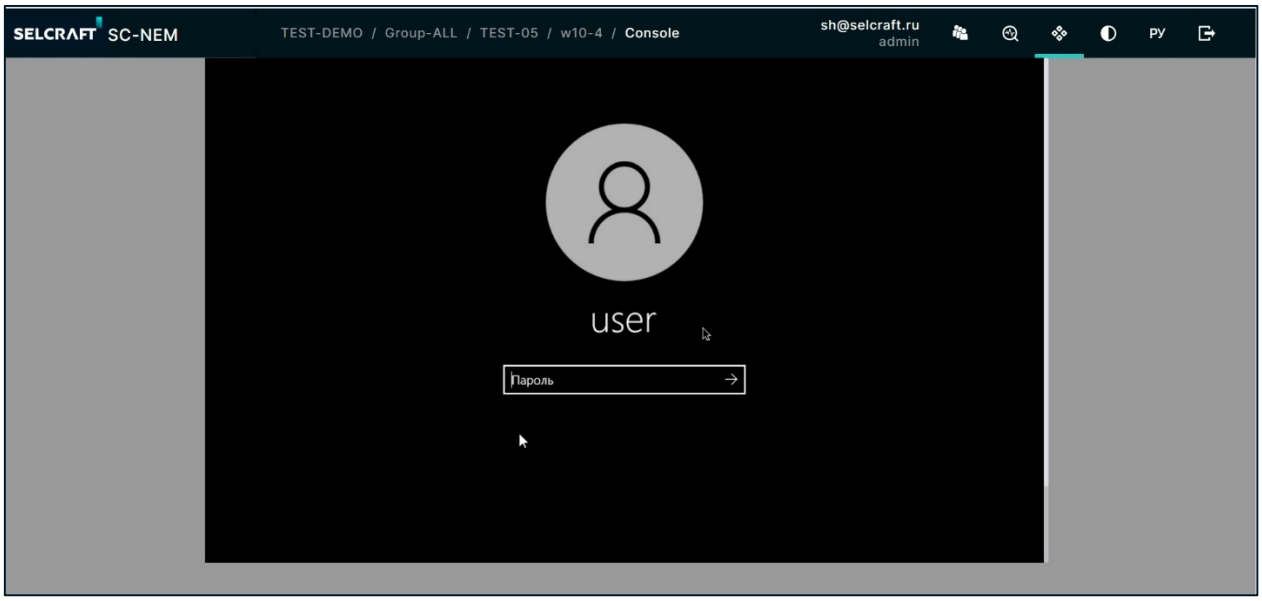
Снимки ВМ – сохраненные текущие конфигурации ВМ/Контейнеров, которые могут быть использованы для создания образов и восстановления ВМ/Контейнеров:



Пользователям доступен легкий доступ к консоли ВМ/Контейнера.

Консоль предоставляет доступ к интерфейсу операционной системы VM/Контейнера. Интерфейс VM|Контейнера может быть графический или текстовый (CLI).

После нажатия соответствующей кнопки консоль или графический интерфейс для данной ВМ будет открыта на отдельной вкладке браузера:

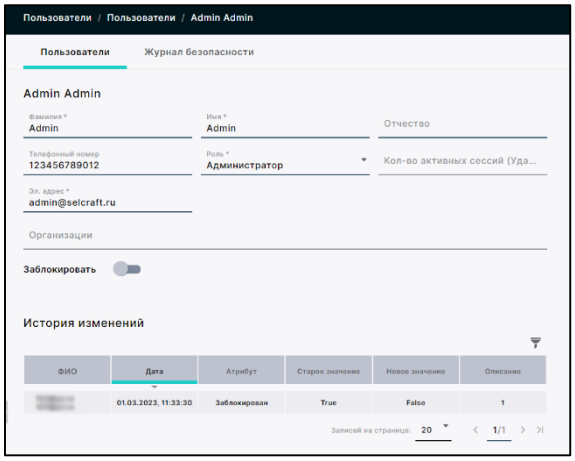


3.6. Управление пользователями – управление пользователями, роли

Система позволяет легко добавлять пользователей и гибко управлять существующими.

Каждый пользователь в системе обладает определенными

- Просматривать список всех существующих пользователей, их основных параметров и текущий статус активности в единой таблице;
- Изменять основные атрибуты пользователей (ФИО, Телефонный номер и тд.);
- Изменять роли пользователей (см. ниже);
- Предоставлять (или ограничивать) доступ пользователей к отдельным Организациям и Группам;
- Настраивать максимальное количество сессий удаленного доступа;
- Блокировать/разблокировать пользователей.



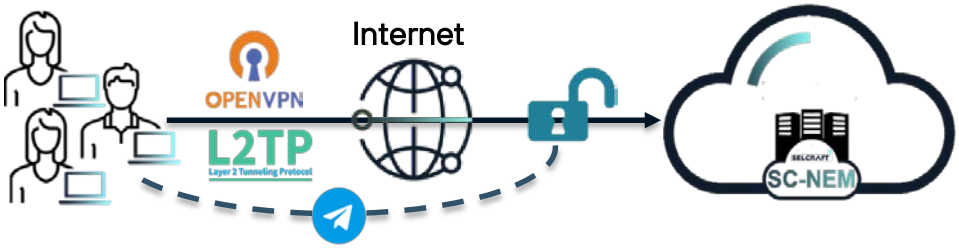
Система предоставляет различный уровень доступа к функциям, в зависимости от роли пользователя. По умолчанию Система предусматривает наличие пяти ролей пользователей:

- Администратор – доступны все функции просмотра и редактирования конфигурации Системы в рамках всех Организаций. Может добавлять и редактировать пользователей в рамках всех Организаций.
- ReadOnly – доступны все функции просмотра конфигурации Системы в рамках всех Организаций.
- Локальный администратор – доступны все функции просмотра и редактирования конфигурации Системы в рамках выбранных Организаций. Может добавлять и редактировать пользователей в рамках выбранных Организаций. Доступна функция удаленного доступа к сетям Организации.
- Локальный Readonly – доступны все функции просмотра конфигурации Системы в рамках выбранных Организациях. Доступна функция удаленного доступа к сетям Организации.
- RemoteAccessOnly – доступна смена пароля. Доступна функция удаленного доступа к сетям Организации.

3.7. Дополнительные возможности

3.7.1. Удаленный доступ к сети

Функционал системы позволяет обеспечить шифрованный контролируемый удаленный доступ/подключение к сетям Организаций с помощью стандартных клиентов OpenVPN, L2TP.



Удаленное подключение пользователя к локальной сети Организации осуществляется через специальный контейнер, разворачиваемый на одном из Узлов Организации.

Для реализации со стороны Организации необходимо выполнить 3 простых действий:

1. Осуществить развертывание контейнера на Узле, используя функционал SC-NEM (Виртуализация). Образ контейнера доступен для установки из облака системы;
2. Осуществить настройку NAT для сети контейнера, используя функционал SC-NEM;
3. Создать удаленную сессию в клиенте OpenVPN или с помощью встроенного функционала Windows (для L2TP).

Шаблон настроек для создания удаленной сессии OpenVPN предоставляются в формате профилей OpenVPN (конфигурационных файлов в формате .OVPN).

В целях усиления безопасности и пресечения попыток несанкционированного доступа к сети, при подключении используется двухфакторная аутентификация (2FA: логин/пароль и подтверждение через мессенджер Telegram).

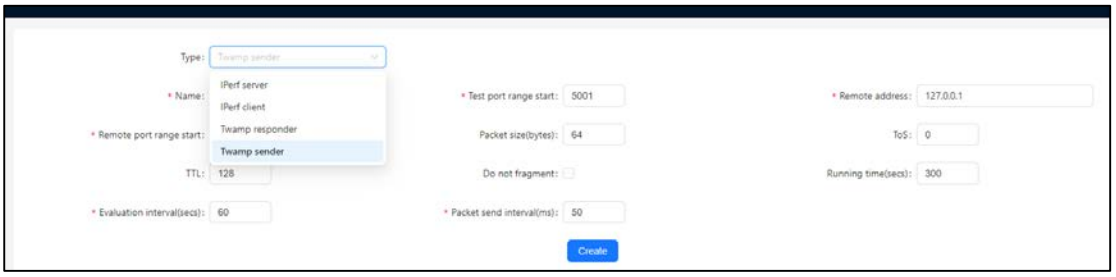
Все попытки подключений пользователей к удаленному доступу журналируются.

Также доступно ограничение доступа к возможности удаленного подключения для конкретных пользователей с помощью GUI. В системе доступно:

- Разрешить/запретить пользователю, удаленный доступ к сетям Организации,
- Ограничить количество единовременных активных сессий для каждого пользователя.

3.7.2. Тестирование подключений, сети

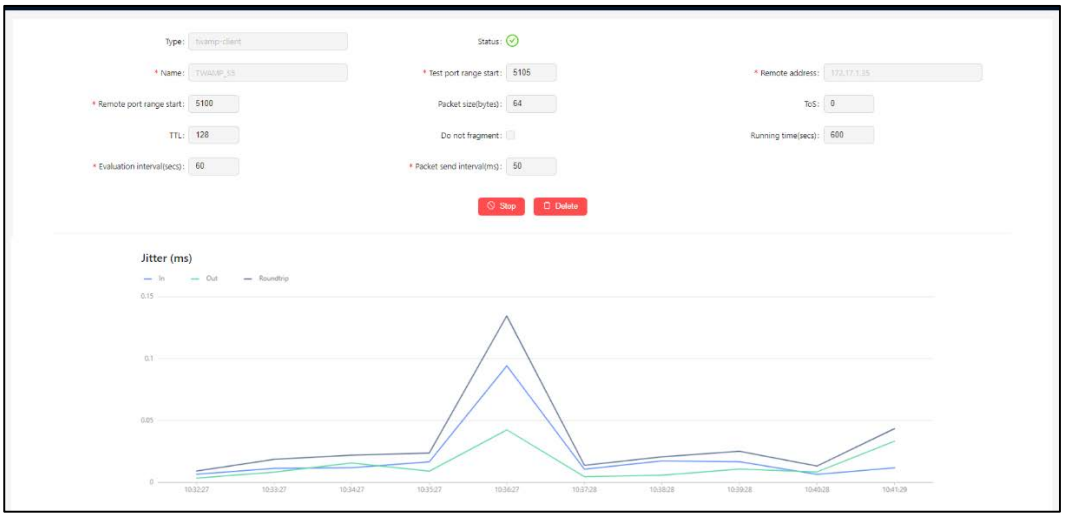
Функционал системы позволяет обеспечить тестирование качества сети. Тестирование качества сети осуществляется через специальный контейнер, который разворачивается на одном или нескольких узлах.



WEB интерфейс контейнера позволят настроить тесты

- Тестирование пропускной способности подключений. Для измерения пропускной способности используется функционал IPERF. Интерфейс позволяет настроить IPERF сервер, клиент и указать необходимые параметры.

- Тестирование качества подключений (потери, задержки, джитер). Для измерения качества каналов связи используется протокол TWAMP.



123112,
Россия, г. Москва,
Пресненская наб. 8 с1

+7 495 123-32-35
info@selcraft.ru
selcraft.ru