SC – NEM

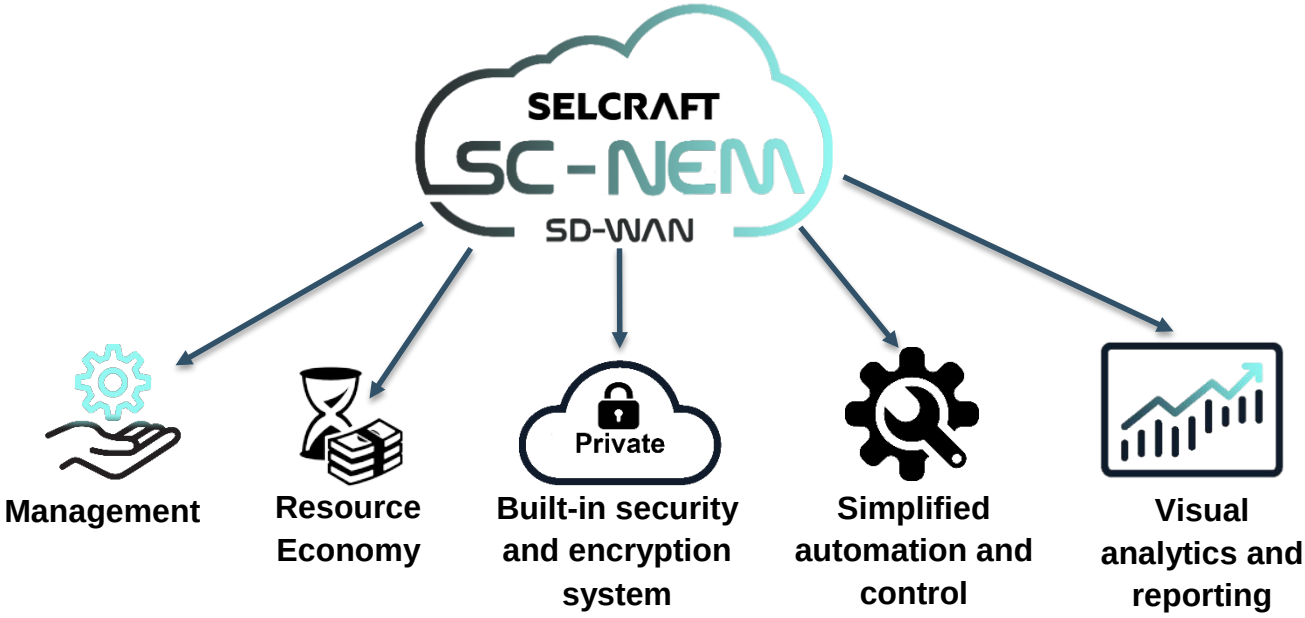
System description

SELCRAFT

Introduction

In modern companies, the primary tasks are increasingly building a reliable corporate network between branches and the head office, and deploying distributed services. At the same time, a natural question arises: how to create and operate such a network and services, effectively manage them and avoid serious failures in their work?

Selcraft offers a modern solution based on software-defined distributed networks (SD-WAN).



1. What is SC-NEM

SC-NEM is a software for universal devices based on x86 and ARM (industrial computers, servers), which provides the ability to deploy and subsequently manage the company's corporate network using an intuitive graphical interface.

Using SC-NEM, you can safely and remotely manage the company's network infrastructure, the traffic of individual organizations, virtual machines and containers, services, as well as monitor networks, virtual machines and equipment.

We continue to modernize our system, improving the functionality and adding a new one.

The full list of available software functions can be found below (Section 1.5).

1.1. What does SC-NEM consist of

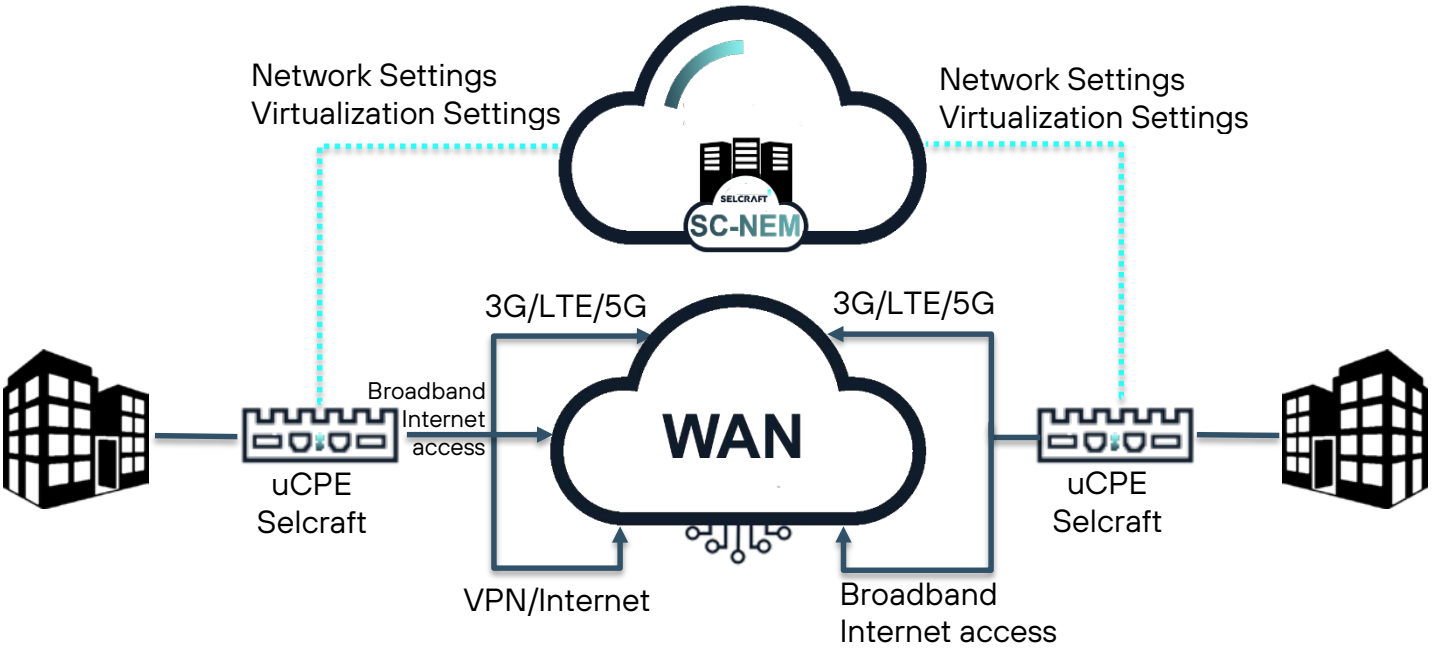
The SC-NEM system consists of the following components:

- External users:
  - Users – administrators and other personnel who work in the system using client workstations;
  - External Systems – OSS/BSS systems.
- External devices:
  - Physical devices – uCPE and similar devices that play the role of Nodes in the construction of network infrastructure;
  - Virtual Machines – VMs and containers deployed on physical devices.
- External services:
  - NTP – synchronization service in the;
  - DNS – Domain Name Service;
  - SSH – remote system management and TCP connection tunneling service.
- Internal components:
  - Controller – the component responsible for applying configurations to Nodes;
  - WEB service – a service that ensures the operation of a WEB application (website);
  - Authentication service – a service that performs the functions of authorizing external users in the system;
  - Monitoring service – a service that performs the functions of providing and storing data on the operation of system components;
  - Asynchronous server – a service that performs functions for the autonomous execution of generated tasks on system components;
  - Database is a service that performs the functions of storing system data and generated tasks;
  - Other components necessary for the implementation of additional functions.

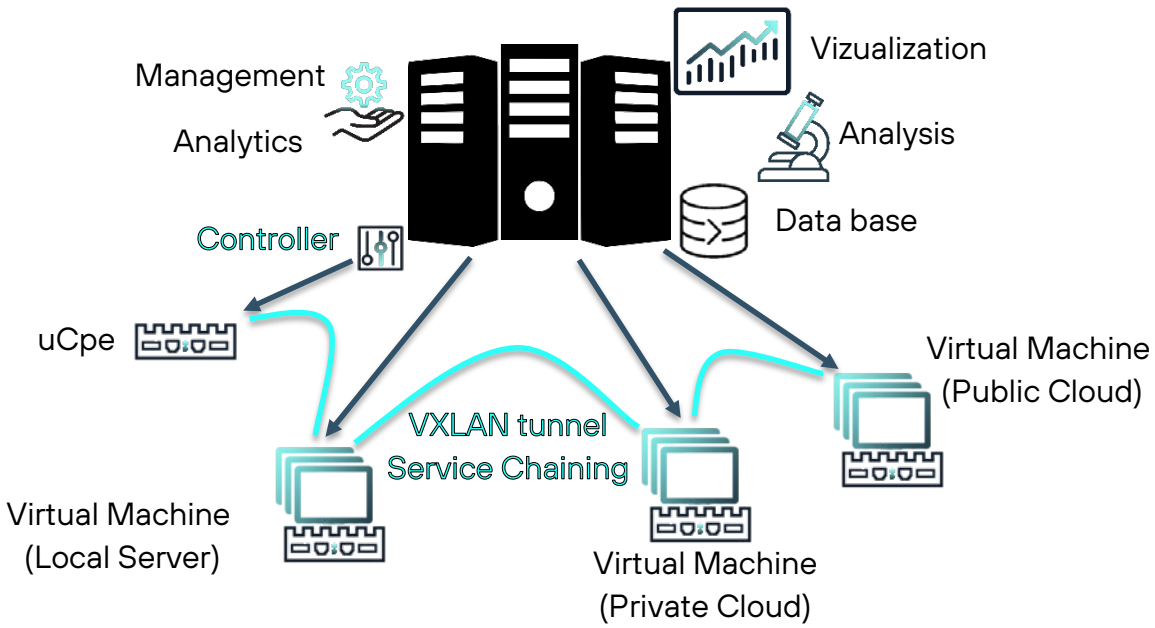
Interaction between External users, External services, Internal and External components of the System is carried out through information flows, through IP protocols.

1.2. What is SC-NEM for?

- Building enterprise-level WAN networks, automating network settings and deploying services:
  - SC-NEM simplifies the implementation of WAN networks and multi-block networks by combining the cloud access policies of regional branches into a single tool. This allows you to segment and reliably isolate the corporate infrastructure consisting of guest wireless communications, business lines, business partners and much more.



- Building a hybrid Cloud Native network:
  - SC-NEM gives access to work with multiple clouds (local, private, public), to ensure connectivity and build a WAN network in accordance with corporate rules. It is possible to install the software on both a physical uCPE and a virtual machine.



1.3. SC-NEM functionality

Now SC-NEM provides the following set of functionality:

❖ Organization Management:	• Adding Organizations; • Editing attributes of Organizations; • Linking Nodes to an Organization; • View a list of existing Node configuration templates and their parameters; • Managing local and public images; • Management of the Organization's L2 VPN and L3 VPN topologies; • View the history of topologies application • Configuring IP settings; • Adding logical routers; • Management of IP ranges of logical routers; • Access Sheet Management (ACL); • Configuring licensing settings; • Configuring security settings; • Configuring the parameters of the monitoring data warehouse and event logs; • View the history of System Settings application (licensing, security, storage) • Configure monitoring parameters; • View the history of the application of monitoring settings; • Viewing messages about the work of the Organization's Nodes; • View statistics about the work of the Organization's Nodes.

❖ Group Management:	• Adding Groups; • Editing Group attributes; • Binding nodes to a Group; • Management of L2 and L3 VPN Group topologies; • View the history of topologies application; • Viewing messages about the work of Group Nodes; • View statistics about the work of the Nodes of the Group.
❖ Node Management:	• Editing Node attributes; • Moving a Node between Organization/ Groups; • Adding (creating) VM/Containers on the Node; • Deleting VM/Containers; • View statistics about the operation of VM/Containers; • Applying the current Node configuration to the System; • View current Node configurations; • View applied and early Node configurations; • Comparison of current and applied Node configurations; • Canceling changes to the current Node configuration; • Creating a template from the current Node configuration; • Restoring the current Node configuration from earlier configurations; • View the history of applied configurations • Viewing Node operation messages; • View statistics about the operation of the Node.

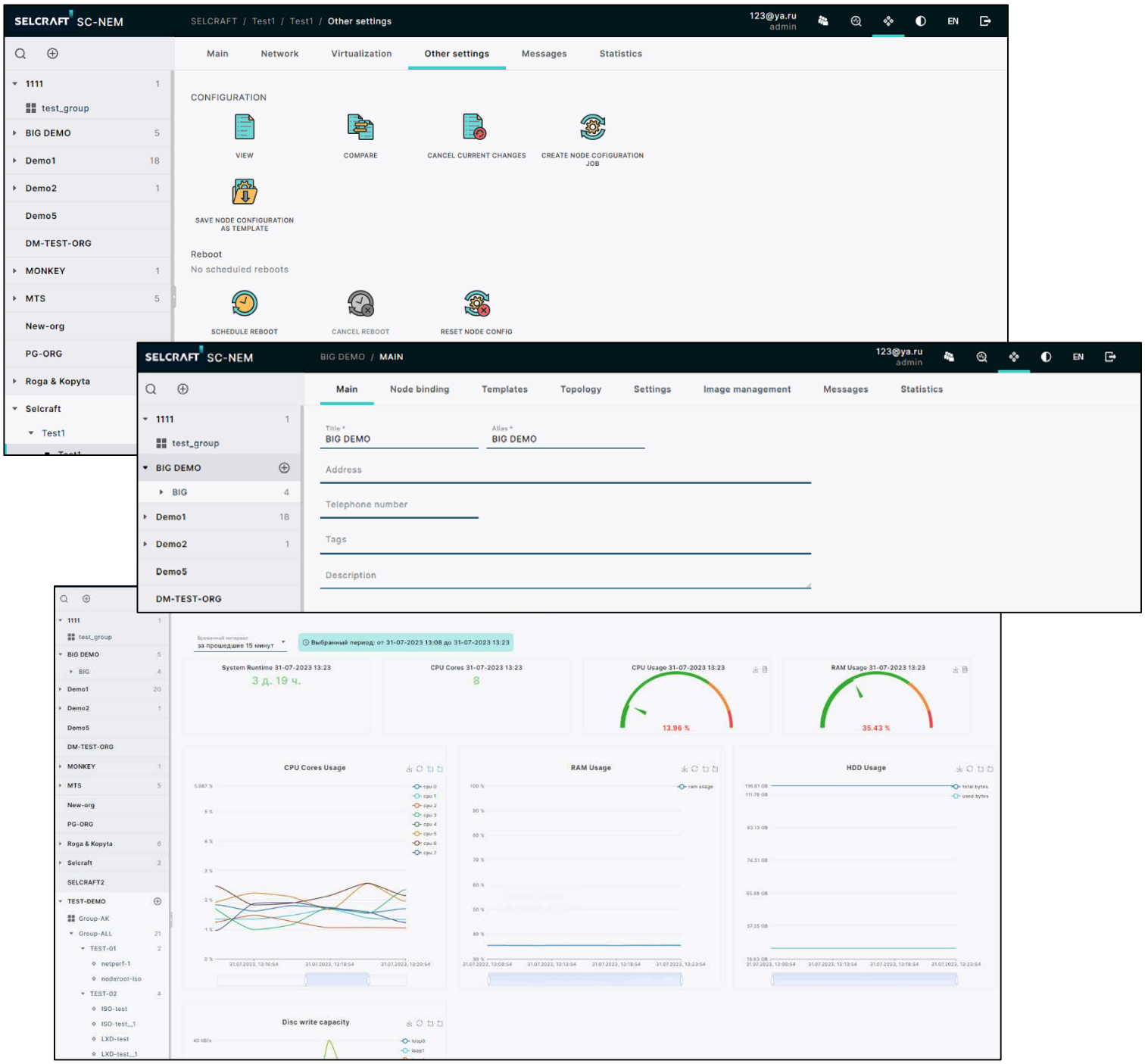
❖ Managing the network settings of the Node:	• Creating, editing and deleting networks; • Configuring DHCP; • VRRP Setup; • WAN connection management; • Configuring the configuration of WiFi endpoints; • Configuring the NAT configuration; • Configuring Routing Configuration; • Configuring the configuration of Rate-Limit, Route-Map, SPAN, QoS rules; • View statistics on the operation of the Node's network interfaces.
❖ Managing Virtual Machines and Containers:	• Editing VM/Containers attributes; • Starting and stopping VM/Containers; • Access to the VM/Containers console; • Creating VM/Containers snapshots; • Creating images from VM/Containers snapshots; • VM/Containers recovery from snapshots; • Viewing VM/Containers operation messages; • View statistics about VM/Containers operation.
❖ User Management:	• Adding users; • Editing user attributes; • Blocking users; • View the history of successful and unsuccessful user login attempts; • Reset/restore/change the password by the user.
❖ Additional features:	• Creation of conditions for remote access to local networks of Organizations; • Initial configuration of the Node via the command line; • Network bandwidth testing using Netpref.

2. User Interface

User Interface (GUI) is complex a of interactive graphical elements grouped into specific Functional Groups located on separate web pages.

Access to the pages is carried out using the HTTPS protocol and a web browser, which allows you to access the System functions from any device that has access to the company's network.

The GUI design is designed to seriously facilitate and speed up the process of adapting Users to work with the SC-NEM System.

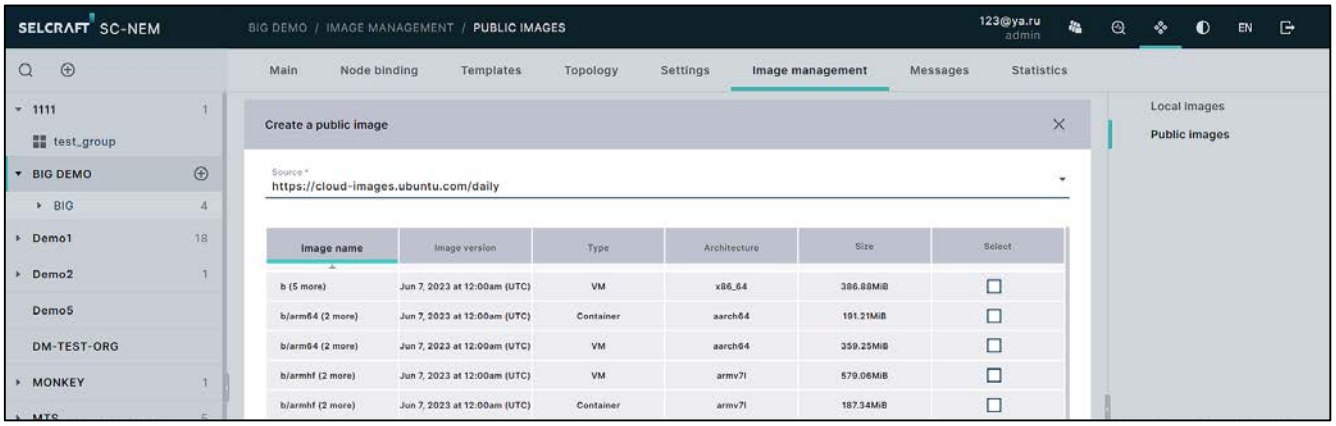


3. Detailed description of some of the available functions

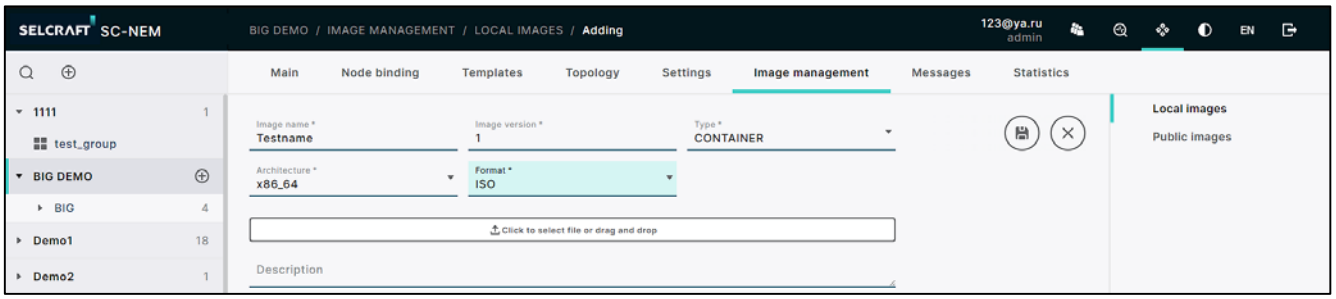
3.1. Organization Management – local and public images

The functionality of the system allows you to use images - saved configurations of Virtual machines and Containers. To deploy a VM/Container using an image, it must be added to the Organization.

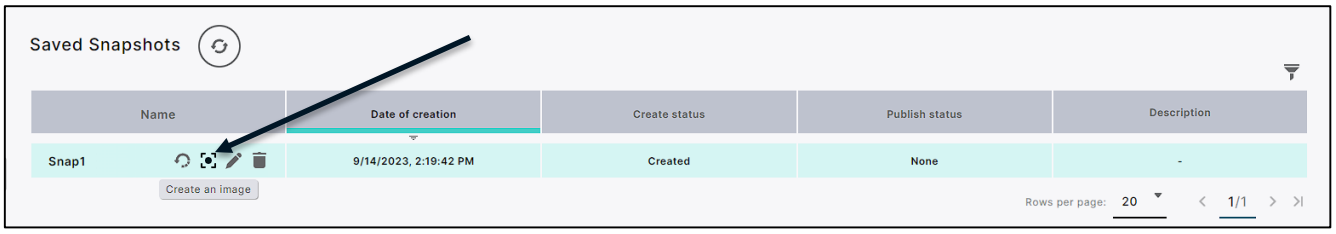
Public - added to the Organization from public sources available to all Organizations:



Local – added to the Organization manually, using a configuration file:



Or they are created from snapshots of VM/Containers belonging to this Organization:



3.2. Group Management – L2 VPN and L3 VPN topologies

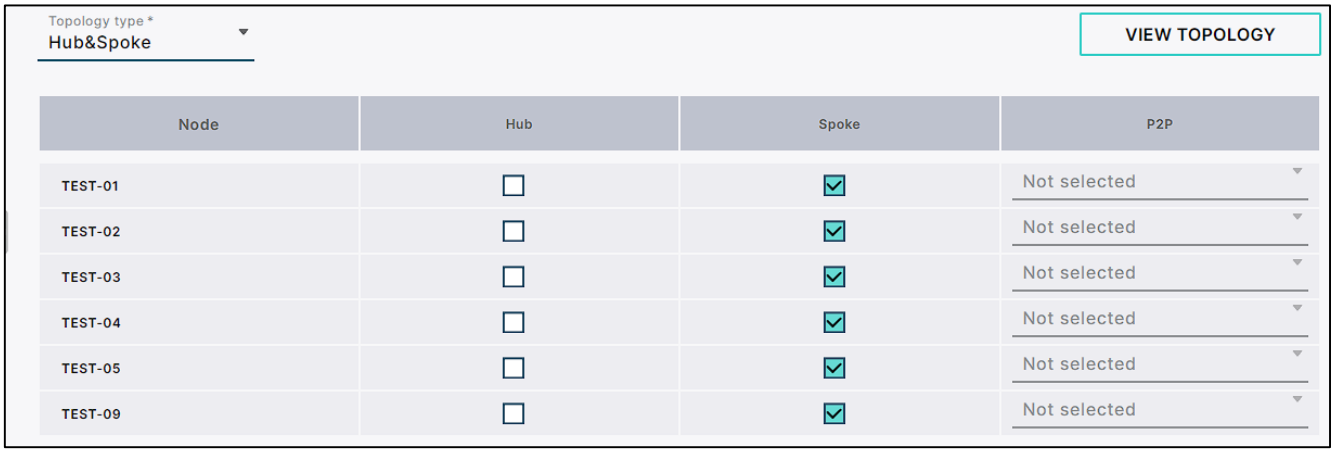
The functionality of the system allows you to manage the topologies of virtual (VPN) connections of Nodes in Groups (and Organizations) for the L2 and L3, respectively.

L2 topologies are based on Nodes local networks, L3 – on logical router connections (VRF).

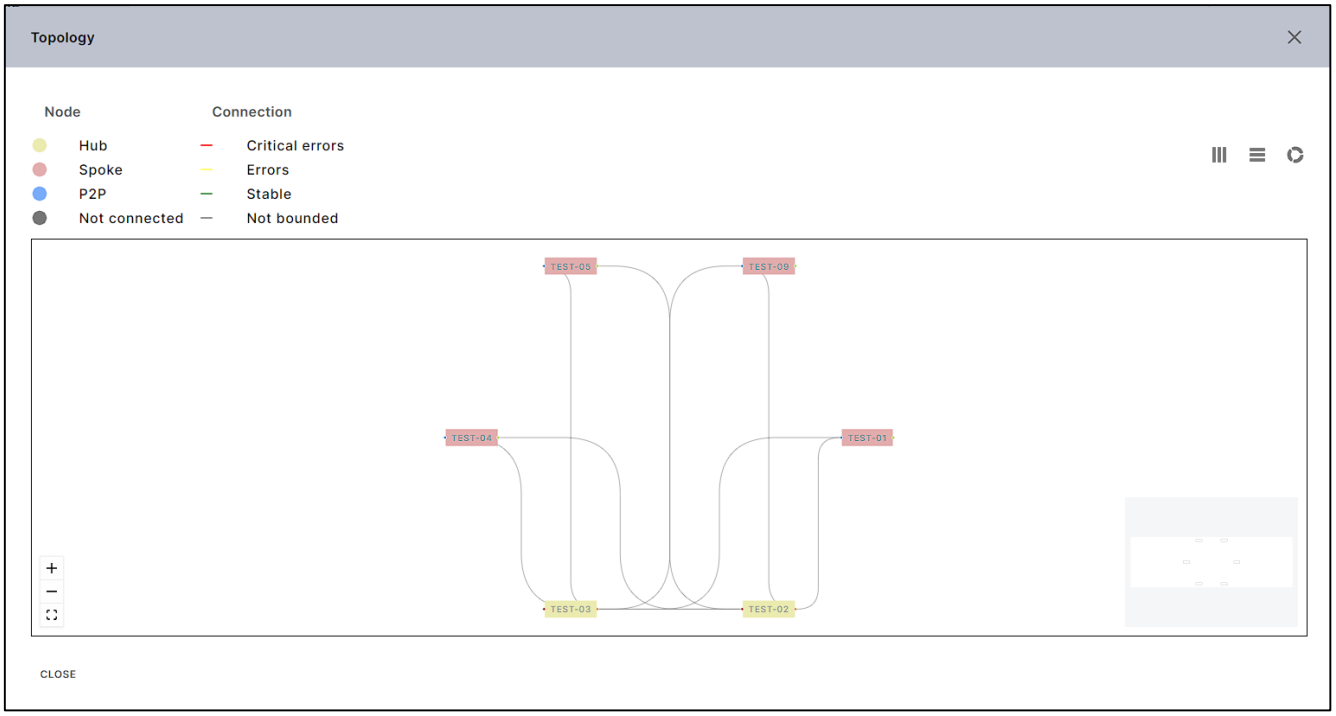
All topologies can be built according to the three main types of Full Mesh, Hub&Spoke and Point-to-Point.

The system provides a function for selecting the type of VPN connection tunnels and the type of VPN encryption.

When adding/editing, the user can include/exclude Nodes from the topology, select their type in the topology, and create a P2P pair for each of the Nodes:



The user can also view the created topology in graphical format:

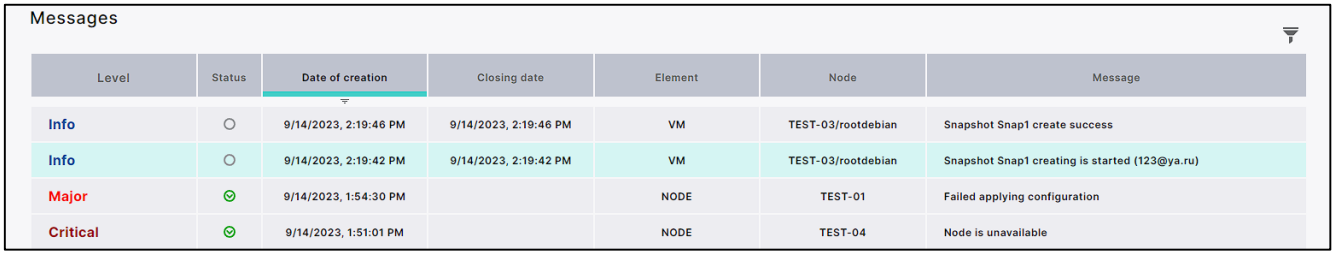


3.3. Node Management - messages and statistics about VM/Containers

The functionality of the system allows monitoring the operation of VM/Containers deployed on a single Node. (Similar functionality is available for monitoring the overall operation of Nodes in Organizations/Groups, individual components of Nodes, and other internal components of the system).

To do this, the user can view server messages and statistics in graphical form.

Server messages are generated automatically and contain information about errors that have occurred during operation, as well as the status of the settings application, and other information:



Statistics are presented in the form of graphs and reflect the statuses of the components in real time. For example, the percentage of CPU utilization of the Node or uptime:

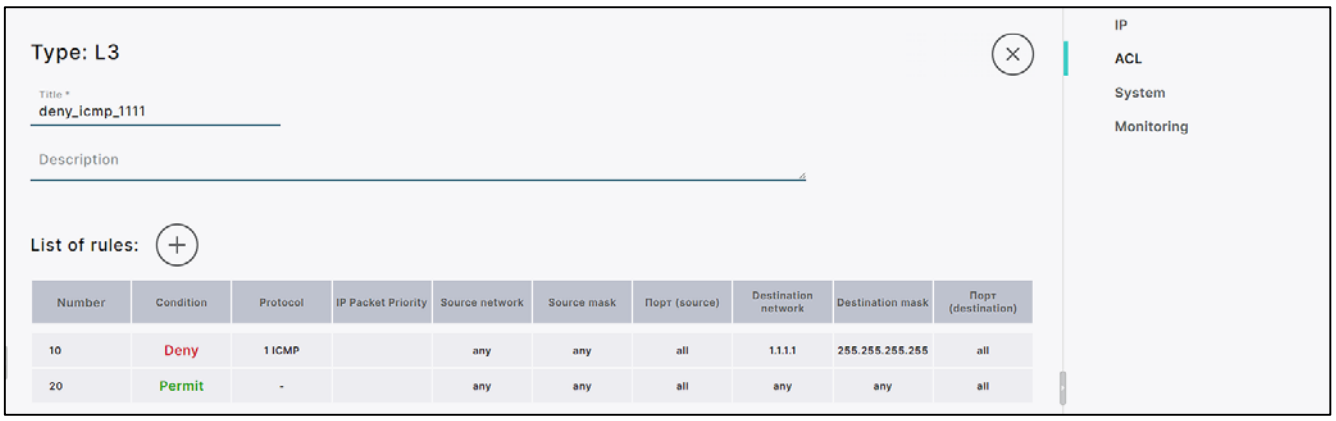
When viewing statistics, you can select the time interval for which statistics are presented.

3.4. Managing network settings of Nodes – rules

The system allows you to configure rules for traffic passing through the Node network.

The functionality includes setting up rules:

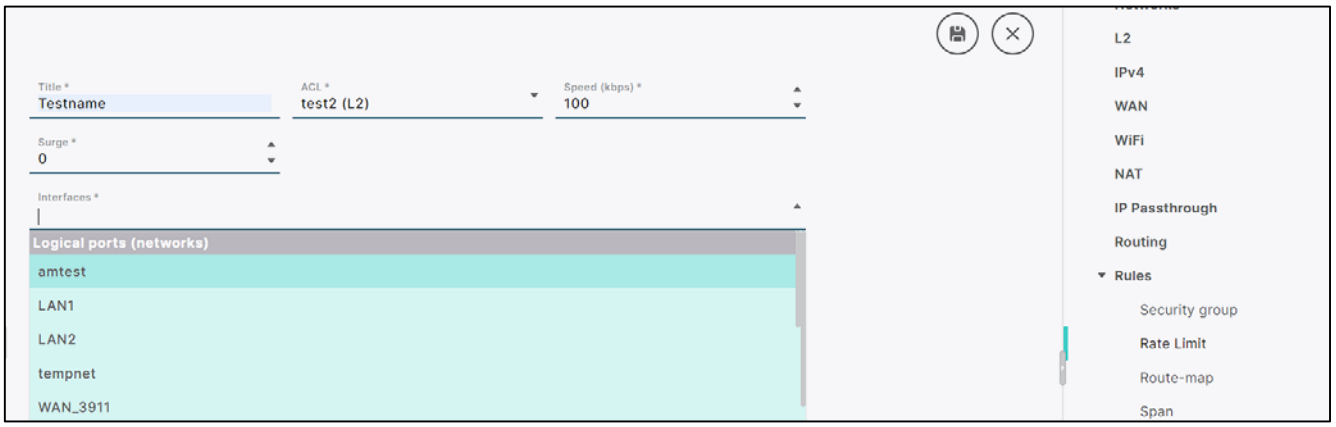
Access Control List (ACL) - management access sheets that define which networks can be used for data packet transmission rules:



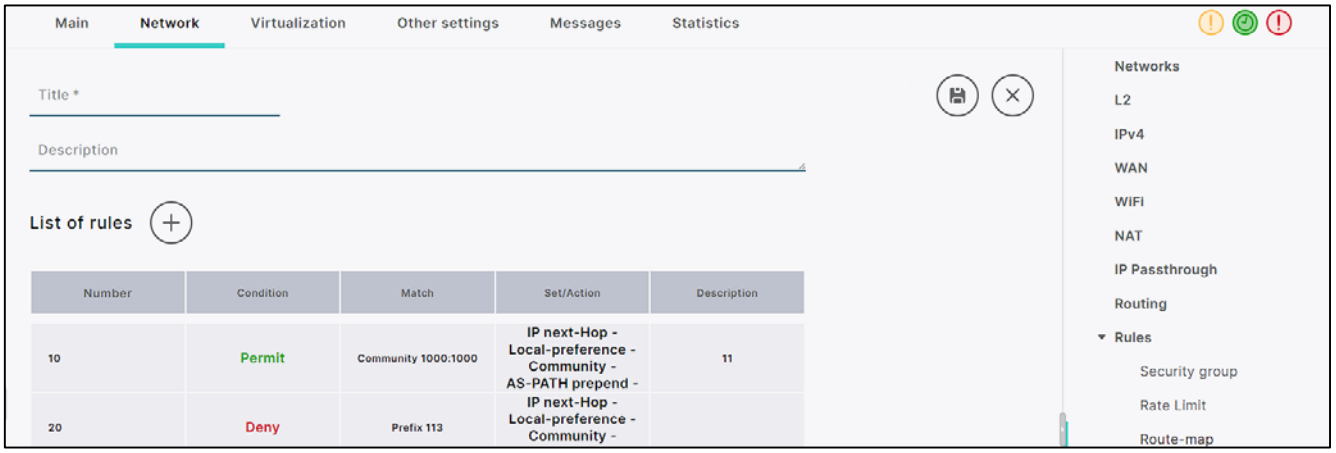
ACLs are part of the Organization parameters and are used when setting up other rules on Nodes.

Security group - network or group of networks to which ACL restrictions apply.

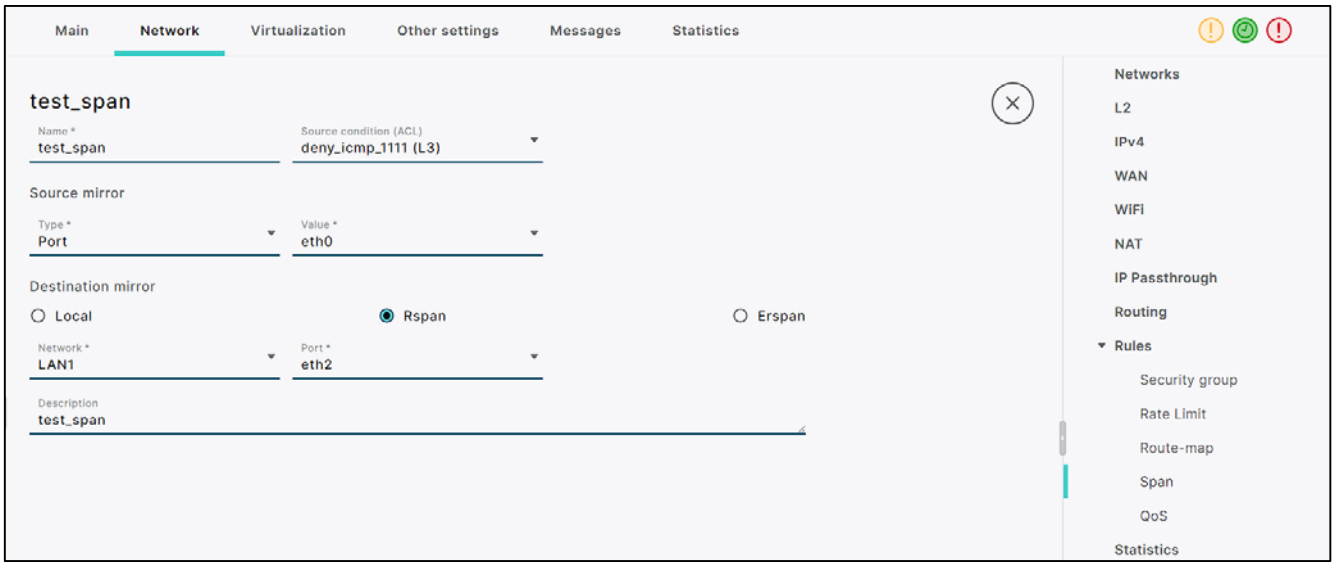
Rate Limit – rules for limiting the data transfer rate between networks:



Route-map – rules for filtering routes and applying various attributes to routes:

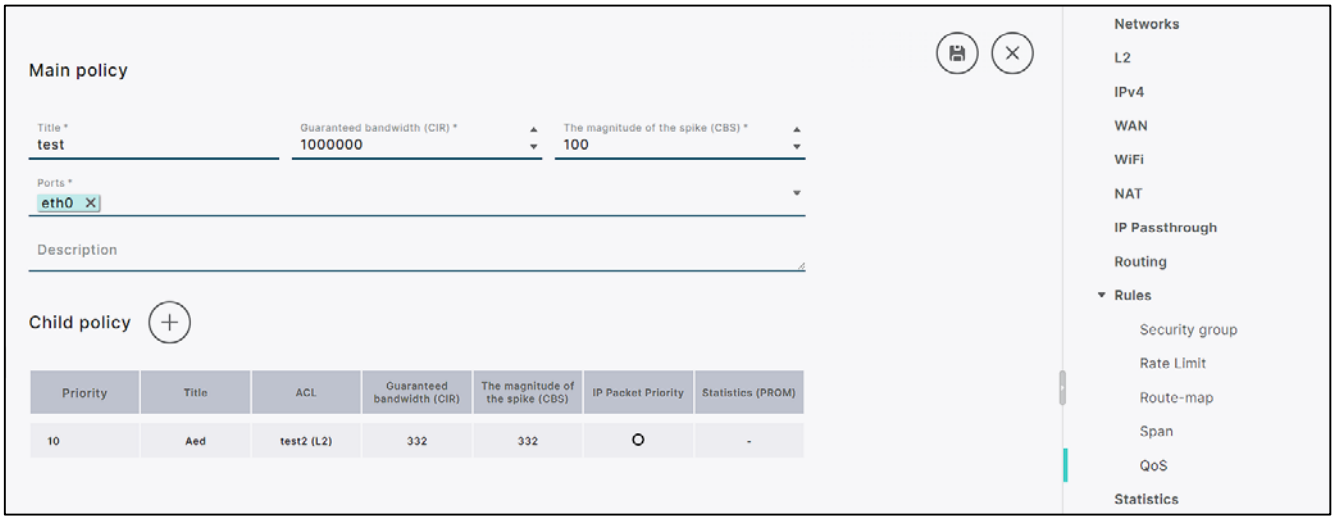


SPAN/RSPAN/ERSPAN – traffic mirroring rules:



These rules allow you to configure the router so that all packets coming to one port or a group of ports of this router are duplicated on another, for the purpose of their further analysis and monitoring:

Quality of Service (QoS) – rules for providing service priorities for different types of traffic:

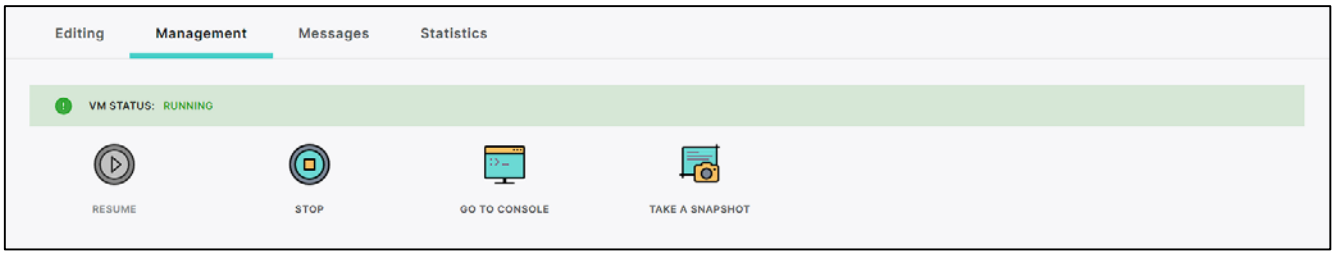


For QoS, it is possible to create main and child policies. The main policy applies to all traffic passing through the selected ports of the Node, the child ones – to parts of this traffic.

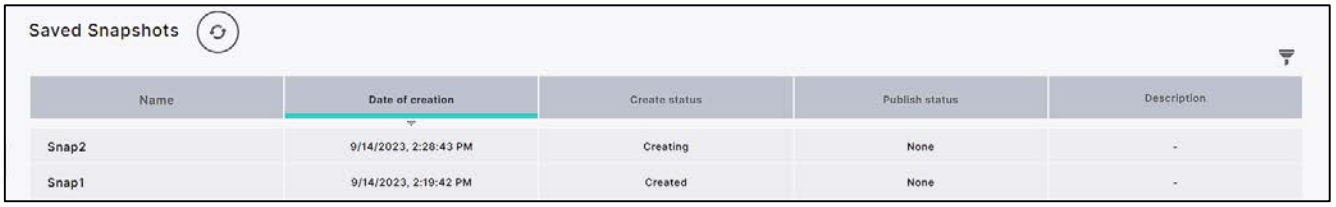
3.5. VM/Containers Management – stop/start, snapshots, console

The functionality of the system makes it easy to manage deployed VM/Containers from the GUI.

The user can stop and start the VM, open the console, create snapshots:



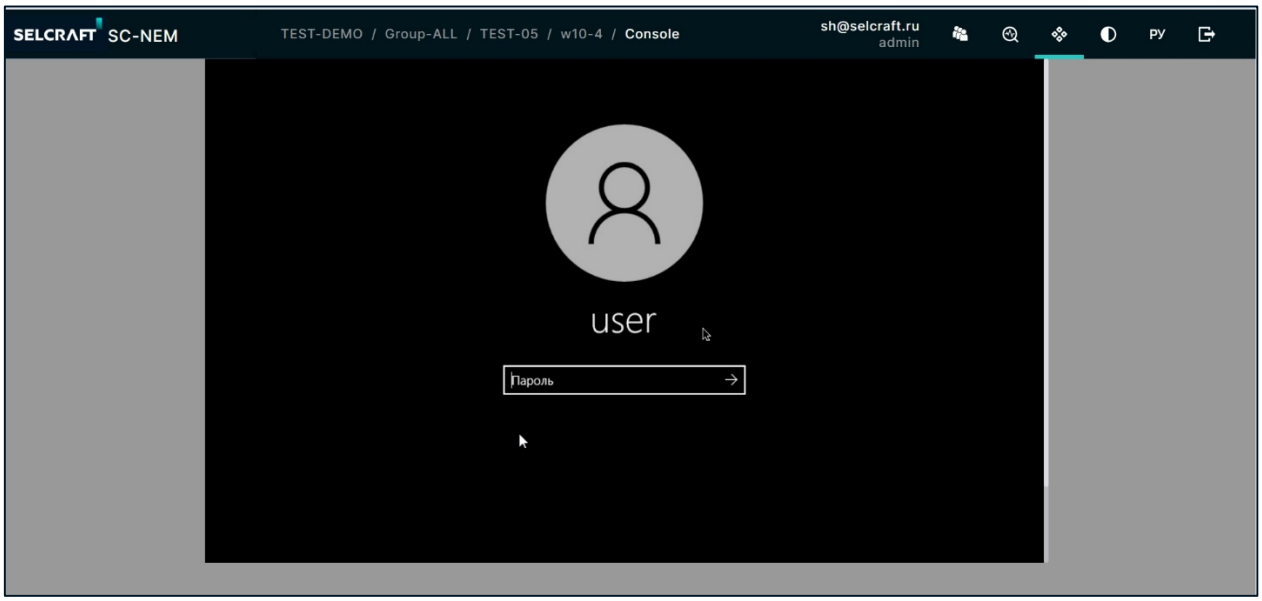
VM Snapshots – saved current VM/Containers configurations that can be used to create images and restore VM/Containers:



Users have easy access to the VM/Containers console.

The console provides access to the interface of the VM/Container operating system. VM /Containers interface can be graphical or text (CLI).

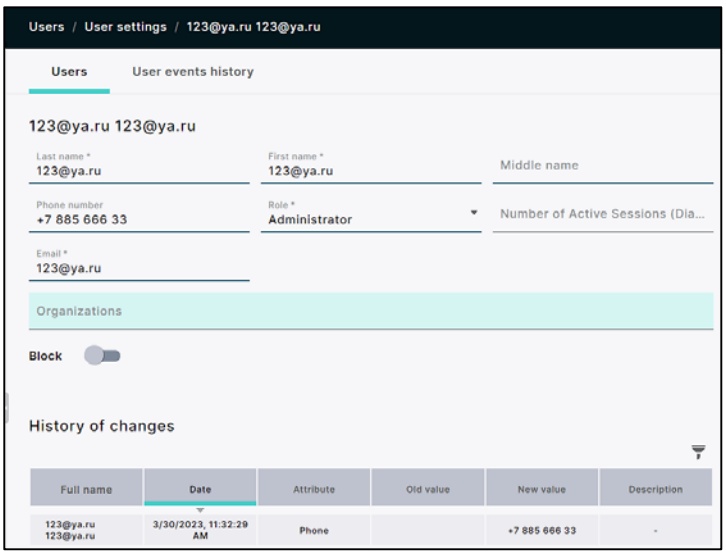
After clicking the appropriate button, the console or graphical interface for this VM will be opened on a separate browser tab:



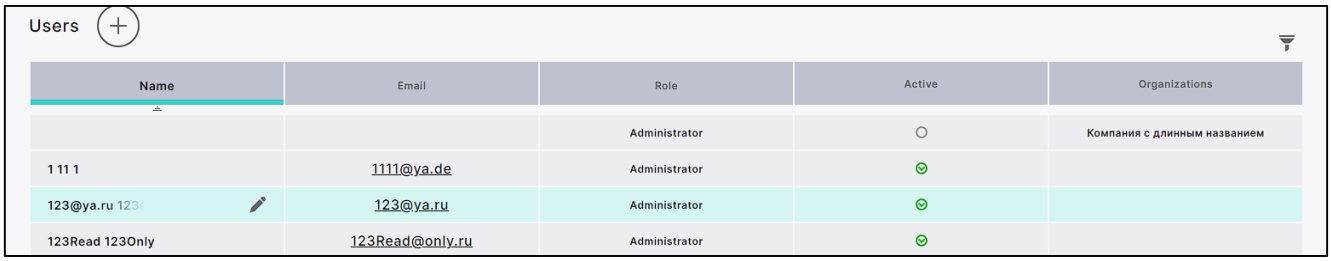
3.6. Users Management – attributes, roles

The system makes it easy to add users and flexibly manage existing ones.

Each user in the system has certain



- View a list of all existing users, their main parameters and the current activity status in a single table;
- Change the main attributes of users (full name, Phone number, etc.);
- Change user roles (see below);
- Grant (or restrict) user access to individual Organizations and Groups;
- Configure the maximum number of remote access sessions;
- Block/unblock users.



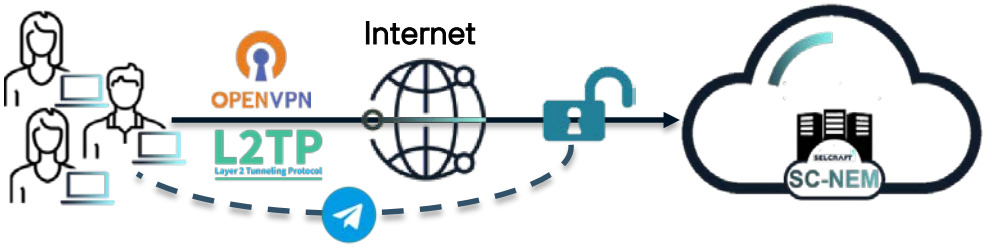
The system provides different levels of access to functions, depending on the user's role. By default, the System provides for five user roles:

- Administrator – all functions of viewing and editing the System configuration within all Organizations are available. Can add and edit users within all Organizations;
- ReadOnly – all System configuration viewing functions are available within all Organizations;
- Local Administrator – all functions of viewing and editing the System configuration within the selected Organizations are available. Can add and edit users within selected Organizations. The function of remote access to the Organization's networks is available;
- Local Readonly – all functions of viewing the System configuration within the selected Organizations are available. The function of remote access to the Organization's networks is available;
- RemoteAccessOnly – password change is available. The function of remote access to the Organization's networks is available.

3.7. Additional features

3.7.1. Remote access

The functionality of the system allows you to provide encrypted controlled remote access /connection to the networks of Organizations using standard OpenVPN, L2TP clients.



The remote connection of the user to the local network of the Organization is carried out through a special container deployed on one of the Nodes of the Organization.

To be implemented by the Organization, it is necessary to perform 3 simple actions:

1. Deploy the container on the Node using the SC-NEM (Virtualization) functionality. The container image is available for installation from the system cloud;

2. Configure NAT for the container network using the SC-NEM functionality;

3. Create a remote session in the OpenVPN client or using the built-in Windows functionality (for L2TP).

The settings template for creating a remote OpenVPN session is provided in the format of OpenVPN profiles (configuration files in the format .OVPN).

In order to enhance security and prevent attempts of unauthorized access to the network, two-factor authentication is used when connecting (2FA: login / password and confirmation via Telegram messenger).

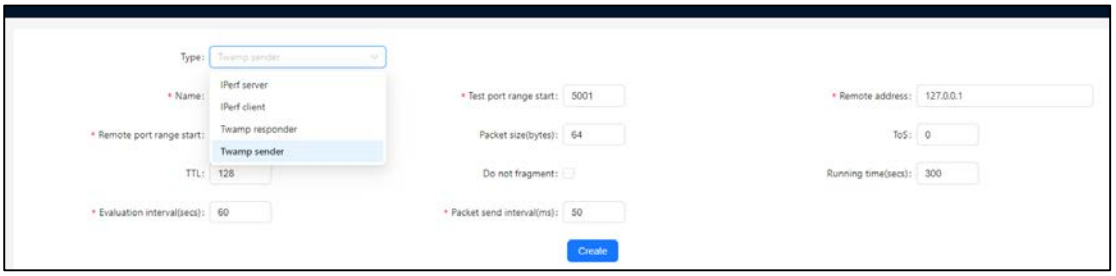
All attempts to connect users to remote access are logged.

Also it is possible to restrict access to the remote connection capability for specific users using the GUI. Available in the system:

- Allow/deny the user remote access to the Organization's networks;
- Limit the number of one-time active sessions for each user.

3.7.2. Testing connections, networks

The functionality of the system allows you to provide network quality testing. Network quality testing is carried out through a special container that is deployed on one or more nodes.



The WEB interface of the container will allow you to configure tests:

- Testing the connection bandwidth. The IPERF functionality is used to measure throughput. The interface allows you to configure the IPERF server, client and specify the necessary parameters.

- Testing the quality of connections (losses, delays, jitter). The TWAMP protocol is used to measure the quality of communication channels.