Connectivity Suite Documentation

Maurin Vögeli

Aug 30, 2022

CONTENTS

User Manual for software version 2.6.x

Modification date: 01.11.2021

Legal Considerations

Content

CHAPTER

ONE

GLOSSARY

1.1 Abbreviations

VPN	Virtual Private Network
OTA	Over the Air
SSH	Secure Shell
AWS	Amazon Web Services
REST	Representational State Transfer
API	Application Programming Interface
UI	User interface
CLI	Command Line interface
NM	NetModule
FQDN	Fully Qualified Domain Name
HMI	Human Machine Interface

1.2 System architecture network overview

The following figure shows the main components that constitute the Connectivity Suite and its associated networks. Please refer to the Section 1.3 in the subsequent chapter for a short description of these components.

1.3 Terminology

1:1 NAT: 1:1 NAT (Network Address Translation) is a mode of NAT that maps one internal address to one external address each. 1:1 NAT is used on every Tenant; it can also be enabled on a Device if required. 1:1 NAT on Tenants allows using the same address space for multiple Tenant subnets. 1:1 NAT on a Device behaves likewise, thus making it possible to access its End Devices via the Connectivity Suite VPN network (Service Access).

Configuration: Refers to the configuration package of a NM router, this package contains at least a user-config.cfg file which contains the main configuration parameters. A configuration package can also contain certificates, user-defined scripts and more. What we commonly refer to as a "router configuration" or simply "configuration" is a ZIP file consisting of

- a text file (user-config.cfg) containing the actual NM router configuration parameters
- a tar archive containing, amongst others, keys and certificates, VPN configurations, SDK scripts

It's the same format you get when you download a NM router configuration via the web interface of the NM router.

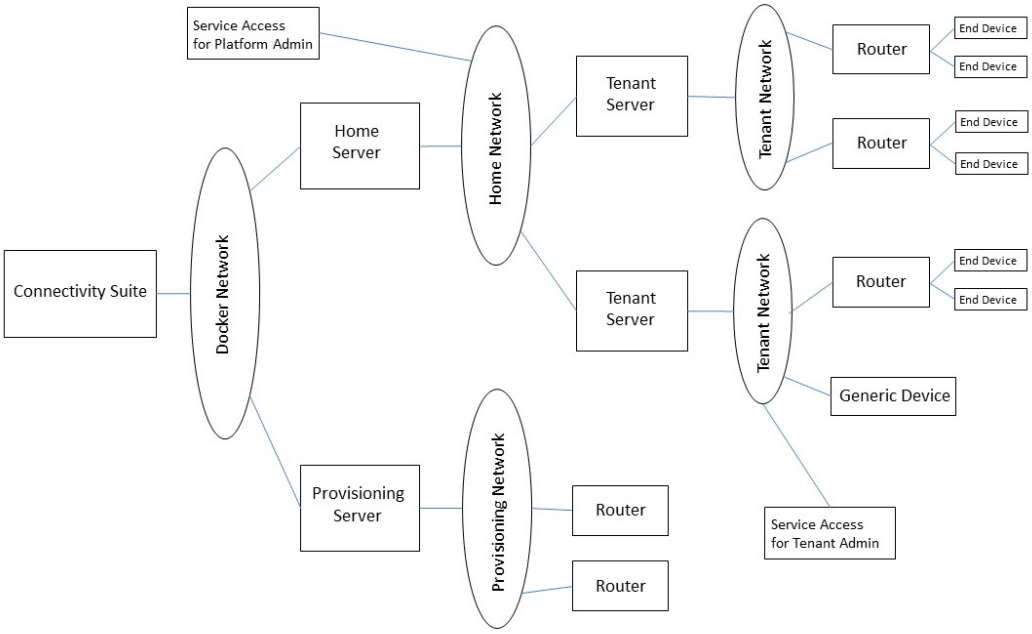

Fig. 1.1: Main components network architecture

Connectivity Suite: The software consists of several microservices, each of which is running as an individual Docker container.

Core Network: The Core Network is used for Docker Networks, the Provisioning Server network, and the Home Server network.

Device: Refers to a NM router, third party routers can currently only be monitored through the Connectivity Suite by integrating them as a Generic Device. Configuration or software updates for third party routers are not supported.

Docker Network The network that connects the Docker containers. It also links these containers to the Home Network (see Section 7).

End Device: Every Device which runs behind a NM router and is directly connected to it.

Generic Device: Every Device which can run as an OpenVPN client and is not a NM router.

Gitlab repository: This is the repository from where the Connectivity Suite software can be downloaded to be installed.

Home Network: A VPN subnet consisting of all Tenants. A Connectivity Suite instance has exactly one Home Network (see Section 7).

Home Server: A VPN server which defines the Home Network (see Section 7).

Job: Can be used to deploy complete Configurations, Snippets or Software to Devices. The execution of a Job can be flexibly scheduled.

Service Access: The Service Access is the established VPN tunnel to directly access the End Devices and Devices in the network. The Connectivity Suite allows the user to download VPN configurations and certificates for establishing VPN connections to the Home Server, the Provisioning Server and any Tenant Server. Once a connection from the user's VPN client to the Provisioning or Tenant Server is established, he can access any Device and Generic Device connected to the subnet of the relevant VPN server. If 1:1 NAT is enabled on a Device, End Devices behind this Device

can be accessed this way as well. As every Tenant is attached to the Home Server, a user with a VPN connection to the Home Server has access to every Device and End Device, whatever Tenant they are assigned to.

Snippet: Refers to a subset of configuration parameters taken from a user-config.cfg file. Snippets can be used for configuring specific features of a NM router without having to upload a complete configuration package. A Snippet can consist of one or more configuration parameters.

Software: The software which will be uploaded to the Devices as a software image.

Standard Configuration: A standard configuration is always bound to a specific physical Device. It contains Device-specific information like VPN certificates and SSH keys, therefore it cannot be deployed to any other Device.

Provisioning Configuration: A Provisioning Configuration contains no Device-specific information and can be deployed to an arbitrary number of Devices. A Device equipped with a Provisioning Configuration has the required VPN configuration and certificates to establish a VPN connection to the Provisioning Server.

Provisioning Network: A VPN subnet consisting of Devices newly detected by the Connectivity Suite but not assigned to a Tenant yet. A Connectivity Suite instance has exactly one Provisioning Network.

Provisioning Server: A VPN server which defines the Provisioning Network.

Task: A Job can contain multiple Tasks. A Task is the execution of a deployment per Device.

Tenant: Short term for Tenant Network.

Tenant Network: Name of a VPN subnet consisting of Devices and Generic Devices. Tenants can be used to group Devices. Role privileges for Connectivity Suite users are granted per Tenant. The certificates used for establishing VPN connections are created in an automated fashion (see Section 7).

Tenant Server: A VPN server which defines a Tenant Network.

CHAPTER

TWO

INTRODUCTION

2.1 Key Features

Remote access with one click: Access all connected routers and clients of your routers within seconds via the web interface of the Connectivity Suite.

Configure & Control: Remote execute automated and scheduled remote over-the-air updates and configurations.

Communication via REST API: REST API to access functionalities from the Connectivity Suite via your own platform or application.

Scalable network: Adding new assets to your existing network can be done within a few minutes and without network configuration know-how required.

Organize & Control Access: Grouping assets based on a multitenancy capability with hierarchical access control to group your assets according to customers, regions, teams etc.

End-to-end Security: Auto-setup of encrypted VPN infrastructure for an end-to-end encryption to secure your communication and your network without any user intervention required.

Cloud based or On-Premise installation: Installation and operation is possible in a cloud environment but also on-premise on your in-house servers to keep control of your data.

2.2 System Architecture

System Architecture

The Connectivity Suite provides several interfaces to communicate and a highly scalable architecture to add networks and devices operating it on-premise or in the cloud. The connectivity suite allows to support up to 150 Tenant Networks each running on a virtual VPN server. To communicate the connectivity suite provides several interfaces:

- Machine to machine-based interface (M2M) based on a REST API
- Human to machine interface (HMI) based web interface using different user roles to restrict access on different levels
- VPN access from as example a back office / operation and Control Centre to the Devices and End Devices via VPN servers in the connectivity suite to run customer applications

The Connectivity Suite runs on a Linux server. For every Tenant Network a virtual server will be setup which acts as VPN server using OpenVPN. Connection to the different devices on each Tenant Network can be established via VPN or private APN. However when using a private APN the VPN will exist within the private APN. The VPN tunnels are required so that the Connectivity Suite can establish a connection to the devices and tenants at all. This means that double encryption is used in the private APN. Once for the APN and once for the VPN tunnel.

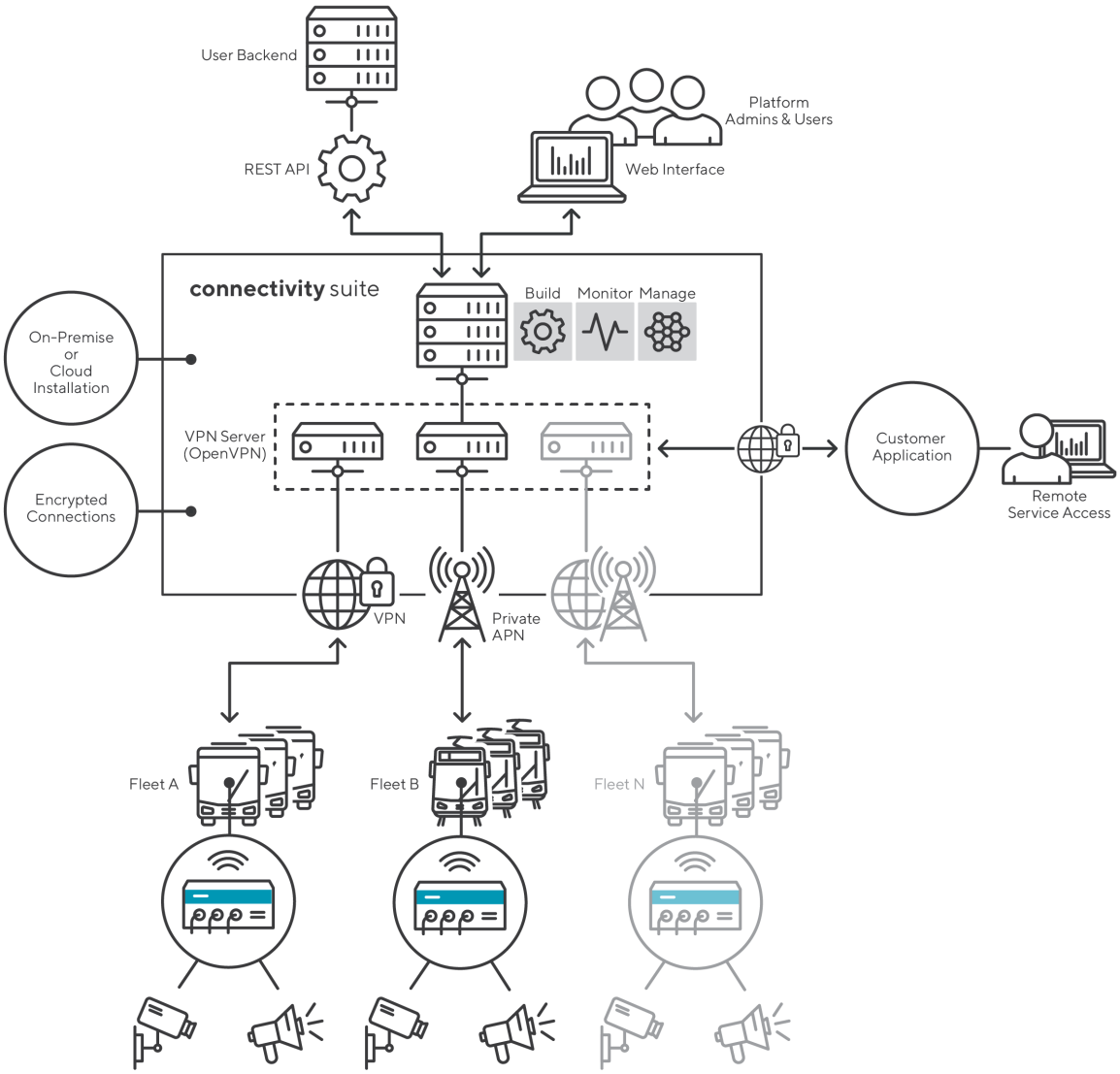

Fig. 2.1: System architecture

2.3 Web interface connectivity suite

The web interface of the connectivity suite provides the interface to configure and setup the connectivity suite incl. the connected devices via a HMI. Find below a description and general overview of the web interface.

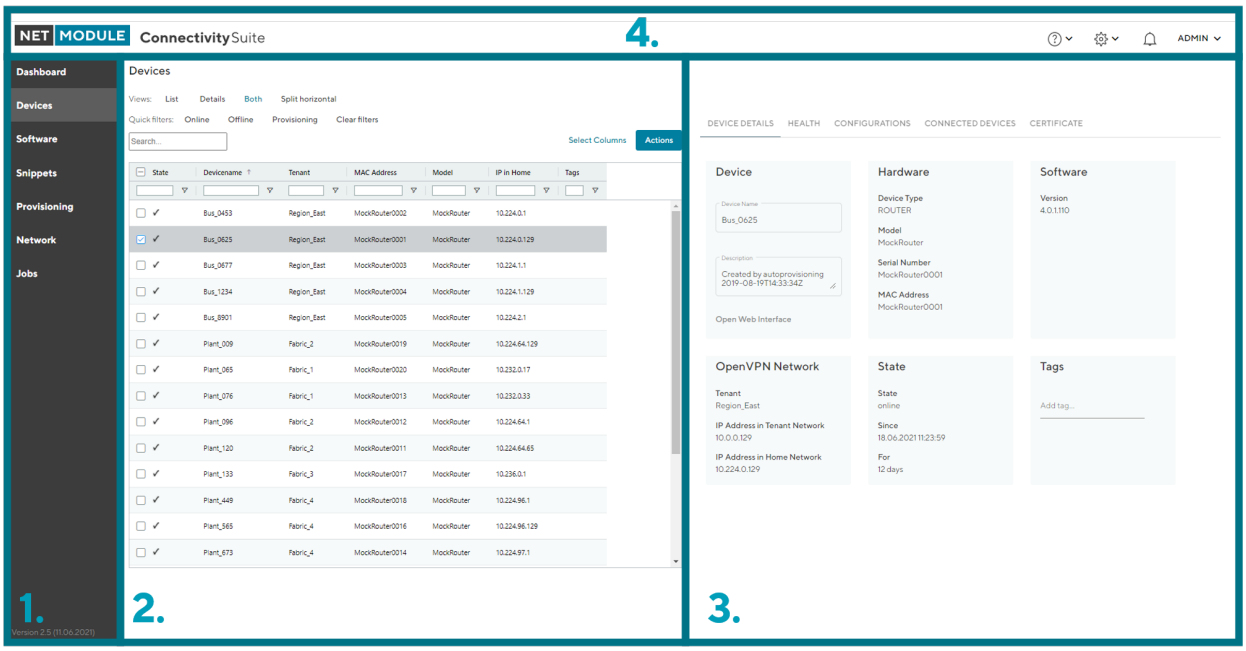

Fig. 2.2: UI overview

1. Navigation bar	2. Main dialogue box	3. Detail dialogue box	4. Support bar
In this bar the navigation between the main features is possible: • Dashboard (application overview) • Devices (overview connected Devices) • Health (overview connection status) • Configuration (configuration management) • Deployment (overview Jobs) • Tenant (overview Tenant)	Provides a table of the different devices, networks, configurations or software versions depending on the page chosen in the Navigation bar.	Provides detailed or requires information about the selection of the Main dialogue box.	Provides general support or help incl. user management.

CHAPTER

THREE

INSTALLATION

Warning: It is assumed that the user who is installing and setting up the Connectivity Suite has read and understood the installation prerequisites (see Section 3.1), otherwise an installation won't be possible.

3.1 Prerequisites

3.1.1 System requirements for a Connectivity Suite instance

Server: Physical or virtual server, either hosted by the company or by an IAAS (Infrastructure as a Service) provider
Operating system: Ubuntu 20, Debian 10
CPU: 2 cores each running at 2.5 GHz
RAM: 16 GB
Disk space: 120 GB
Devices Total: 250 Devices
Tenants Total: 10 Tenants

3.1.2 Supported devices

NB8xx
NB1xxx
NB2xxx
NB3xxx
ES3300

3.1.3 Amount of connected Devices

The number of tenants and devices that can be connected to the Connectivity Suite depends on the hardware resources. The greater the RAM and CPU performance, the more tenants and devices can be connected.

Warning: Insufficient system resources can cause devices to lose connection and Connectivity Suite operation can no longer be guaranteed.

There are two ways to allocate additional resources. One option is that the Connectivity Suite instance gets more RAM and CPU performance or you install remote Tenants to allocate more ressources. Unfortunately, there are no

guidelines on how much to increase system performance per unit. This depends on the operations and functions used on both the Connectivity Suite and devices. This is specific to each installation. The first option is to increase the system resources for the Connectivity Suite instance. The number of devices to be connected depends on the RAM and CPU performance.

Allocate more hardware ressources by increasing server performance

The first option is to increase the system resources for the Connectivity Suite instance. The number of devices to be connected depends on the RAM and CPU performance. If more RAM and CPU performance are made available, more devices can be connected.

Allocate more hardware ressources by adding remote Tenants

The second option is that Tenants are installed on remote servers so that they can access resources from additional servers (see chapter Section 3.1.1 for the installation of a remote Tenant). A dedicated server exclusively used for Remote Tenants can allocate resources only for the Tenant and the devices connected to the tenant. This allows the user to connect significantly more devices to the remote Tenant than to a conventional Tenant as shown in the example below:

CPU: 2 cores each running at 3.6 GHz
RAM: 4 GB
Devices Total: 750 Devices
Tenants Total: 2 Tenants

CPU: 4 cores each running at 3.6 GHz
RAM: 8 GB
Devices Total: 1000 Devices
Tenants Total: 2 Tenants

3.1.4 Domain name

FQDN

- A FQDN is needed which points to the IP address of the server where the Connectivity Suite is installed.
- If you want to use TLS certificates issued by Let's Encrypt, this FQDN must be publicly known and accessible.
- This same FQDN is also used for the routers to connect to the Connectivity Suite as well as for the users to access the Web UI.

Devices CNAME (Subdomain)

To be able to use the web proxy a devices CNAME DNS record is necessary. Example:

Name	Type	Value
devices.cs.mycompany.com	CNAME	cs.mycompany.com

Example

Name	Type	Value
devices.cs.mycompany.com	A	10.42.42.42
devices.cs.mycompany.com	CNAME	cs.mycompany.com

3.1.5 SSH

- Installed OpenSSH server on the Ubuntu server
- SSH on the devices must be enabled and open for OpenVPN tunnels. The Connectivity Suite uses SSH connections via an OpenVPN tunnel to manage the devices.

3.1.6 Network Connections

The server must have access to the internet. Therefore, the following ports must be opened for incoming connections to the server:

Protocol	Port	Description
TCP	SSH port 1)	For management access (automated deployment of Tenants etc.)
TCP	80 2)	Certbot (for certificate renewal)
TCP	443 3)	Tyk Gateway (for accessing the API)
UDP	1194 4)	OpenVPN Home Server
UDP	1195 4)	OpenVPN Provisioning Server
UDP	Custom 4)	OpenVPN Tenant Servers (one port per Tenant)

1) Loopback connections must be allowed for the ports TCP 22 and TCP 443 (i.e. the server must be able to establish SSH and HTTPS connections to itself using its FQDN).

2) Only required if you want to use TLS certificates issued by Let's Encrypt.

3) If all the users of the Connectivity Suite UI are located inside the company network, port 443 need not be opened to the outside world.

4) If all the routers managed by the Connectivity Suite are located inside the company network, these UDP ports need not be opened to the outside world.

Note: The router through which the Connectivity Suites accesses the internet must support the NAT loopback functionality. If this is not the case, operation of the Connectivity Suite will not be possible. A list of routers that fulfil the functionality can be found at the following link: http://opensimulator.org/wiki/NAT_Loopback_Routers

---

3.1.7 Private subnetworks

Two subnetworks out of the private IP address space are needed. The two subnetworks must not overlap with other private networks in use. The subnetworks will be required during the initialization of the Connectivity Suite (see Section 3.3).

- The first subnetwork is for the Core network, which is used to run the application infrastructure. Its size is fixed to 4096 addresses, i.e. a /20 subnetwork.
- The second one is for the Home network. It contains all the routers, as well as all the end devices connected to them. Choose it large enough, as it cannot be enlarged later. Its size can be roughly estimated like this:
  - If there is no need to access the end devices, the minimum size of the Home network corresponds to the number of routers you want to connect to the CS.
  - If you want to access the end devices behind the routers, the minimum size of the Home network is [number of routers] * [average number of end devices behind a single router].
  - Because the Home network will be divided into several address pools during the installation process, its size cannot be smaller than 4096 addresses (a /20 network).

The image below shows what a system architecture can look like and provides an examples what thoughts have to be made in advance to the installation.

Example system architecture

Note: The Connectivity Suite supports only IPv4 operation in IPv6 networks wont be possible.

3.2 Installing the Connectivity Suite and prerequisites

To be able to run the Connectivity Suite on-premises, several prerequisites must be installed, and the Connectivity Suite must be initialized.

Warning: Only a sudo user can execute installations. Do not install while being logged in as a root user, it wont work.

1. Log into your server where the Connectivity Suite will be installed as a user who has root privileges (superuser)
2. Download the Software from the Connectivity Suite Gitlab repository (for the following steps it is assumed that the folder is named cs). The link and credentials for the Gitlab repository are provided by NM incl. a Read Me Instruction on how to download the software to the server.
3. Run the script cs-install-ubuntu from the cs/scripts folder on the server.
4. After executing the script, the User is prompted to enter the hostname of the server which hosts the Connectivity Suite.
5. The prerequisites are installed, and the latest Docker images are pulled automatically, this step takes some time.
6. If a certificate for the SSL connection exists already you will be prompted to decide if the certificate should be renewed or kept.
7. When prompted, log out.

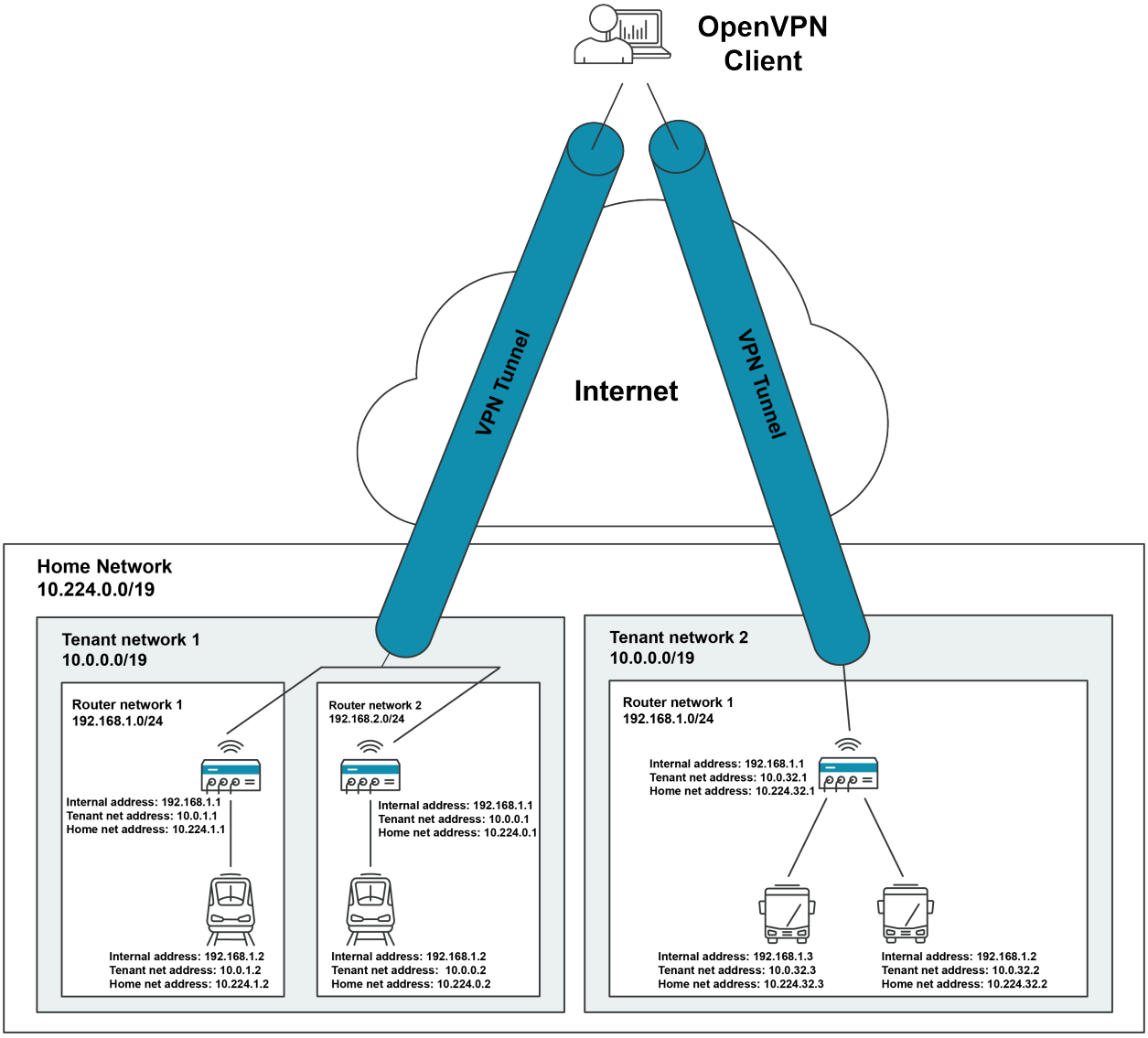

Fig. 3.1: Example architecture

3.3 Initializing the Connectivity Suite

After the installation the Connectivity Suite must be initialized. During this process the Core Network is con-figured. For details regarding the network configuration and layout see Section 7.

1. Log in to your server where the Connectivity Suite has been installed as a user which has root privileges (superuser).
2. Run the script reset-data from the cs/scripts folder.

Warning: Attention! The following steps can only be configured during the installation and are only reversible by doing a re-installation (which means you will lose all the stored data).

3. Configure the Core Network in the format xxx.xxx.xxx.xxx/20. It is mandatory to use a subnet mask of 20 (see Section 7 for more detailed description).
4. Configure the Home Network in the format xxx.xxx.xxx.xxx/xx and make sure the subnet is greater than 20. Also be aware that as example a subnet of 20 does not mean that you will be able to connect 4096 devices there is a big reduction based on the network architecture. (see Section 7 for more detailed description).

Warning: Attention! The Home Network restricts the amount of Devices and End Devices which can be connected to the Connectivity Suite. If the Home Network is too small you wont be able to connect your devices.

5. When prompted choose between default settings for your Network layout or do the settings by yourself. If you choose the default settings step 6-11 can be skipped.

Warning: Only experienced users are allowed to do the settings in step 6-11.

6. Choose your preferred Home Network layout (you have the option of three given layouts).
7. Enter a name for the Tenant type.
8. Enter the number of max. required Tenants. Be aware that if the number set during this step is too small this cannot be changed afterwards.
9. Configure the size of the Tenant, the default network (in the format xxx.xxx.xxx.xxx).
10. Enter the number of max. required End Devices. Be aware that if the number set during this step is too small this cannot be changed afterwards.
11. Enter the number of concurrent Service Access sessions. Be aware that if the number set during this step is too small this cannot be changed afterwards.

Warning: Step 7-11 may need to be repeated, depending on the chosen Home Network layout in step 6.

12. Choose a username for the platform administrator account (see Section 10.4 for the user roles). Wait for the initialization process to finish, this takes a while. Be aware that the username cannot be changed afterwards.
13. Choose if you want Let's Encrypt or the Connectivity Suite certification authority to be used to issue the SSL certificate to access the UI.

Note: If you choose the Connectivity Suite certification authority to issue the SSL certificate, it is not required for port 80 to be open for incoming connections in your firewall! However, your browser is going to display a warning the

first time you open the Connectivity Suite UI. This is normal behaviour. In order to make this warning disappear, your browser needs to trust the Connectivity Suite Root Certification Authority. The procedure varies for different browsers (see Section 3.4).

Note: Note that some domains which are automatically created by providers such as AWS are not accepted by Let's Encrypt and can therefore not be used.

14. As soon as the process is finished, the login data and the address of the Connectivity Suite UI is shown, log into the UI using these credentials.
15. After the first login the user will be requested to change the password.
16. After changing the password, the Connectivity Suite will be ready for use.

3.4 Browser settings Connectivity Suite SSL Certificate

Downloading the Connectivity Suite Root CA certificate using Microsoft Edge

1. Click on Certificate Error to the left of the address bar
2. Choose the Connectivity Suite Root CA from the menu on the right
3. Click on Export to file, this is the file that needs to be imported using one of the import procedures described below

Making your browser trust the Connectivity Suite Root CA

The client operating system or browser now needs to have the CA certificate added to its list of trusted CAs. The instructions vary by operating system and browser but instructions for a few major browsers are listed below.

Client (Operating System, Browser)	Instructions
Microsoft Windows	Right click the CA certificate file and select 'Install Certificate'. Follow the prompts to add the certificate to the trust store either for the current user only or all users of the computer.
Firefox	Firefox does not use the operating systems trust store so the CA needs to be added manually. Manually add certificates and manage added certificates through Firefox's Privacy & Security preferences. More information can be found on Mozilla Wiki
Chrome	If Chrome is configured to use the Windows trust store, adding the certificate to Windows (see above) is sufficient to add trust to the browser as well. Otherwise the certificate can be added manually using the following procedure: Open Settings > Advanced > Manage Certificates > Authorities, and select Import.
Edge/Internet Explorer	Edge/Internet Explorer uses the Windows trust store so adding the certificate to Windows (see above) is sufficient to add trust to the browser as well.

CHAPTER

FOUR

FIRST SETUP

4.1 First Login

When logging into the Connectivity Suite for the first time, a prompt appears stating that no Tenant has been set up yet. To be able to use the Connectivity Suite it is necessary to set up a Tenant. This can be done via the "Network" page. The detailed procedure is described in Section 4.3.

If you don't want to set up the network immediately after your first login you can get to the "Network" page anytime using the Navigation bar.

Warning: If you do not setup a Tenant, you won't be able to assign a router to a network which means that no Jobs can be executed on the Devices.

4.2 First Network Setup

During the automatic network setup process the Home and Provisioning Server are initialized. It can take up to a minute until the Connectivity Suite detects the servers. the initial setup is now completed and the network overview on the page "Network" should look like in Fig. 4.1:

4.3 Adding Tenants to the Connectivity Suite

The Tenants allow logical grouping and separation of several network sites within one management platform. A Tenant ensures that devices within a Tenant can not communicate cross-tenant and therefore grant role privileges for Connectivity Suite users.

To connect routers to the Connectivity Suite it is required to add Tenants as every router needs to be assigned to a Tenant.

For the following steps an account with **Platform Administrator** right is required.

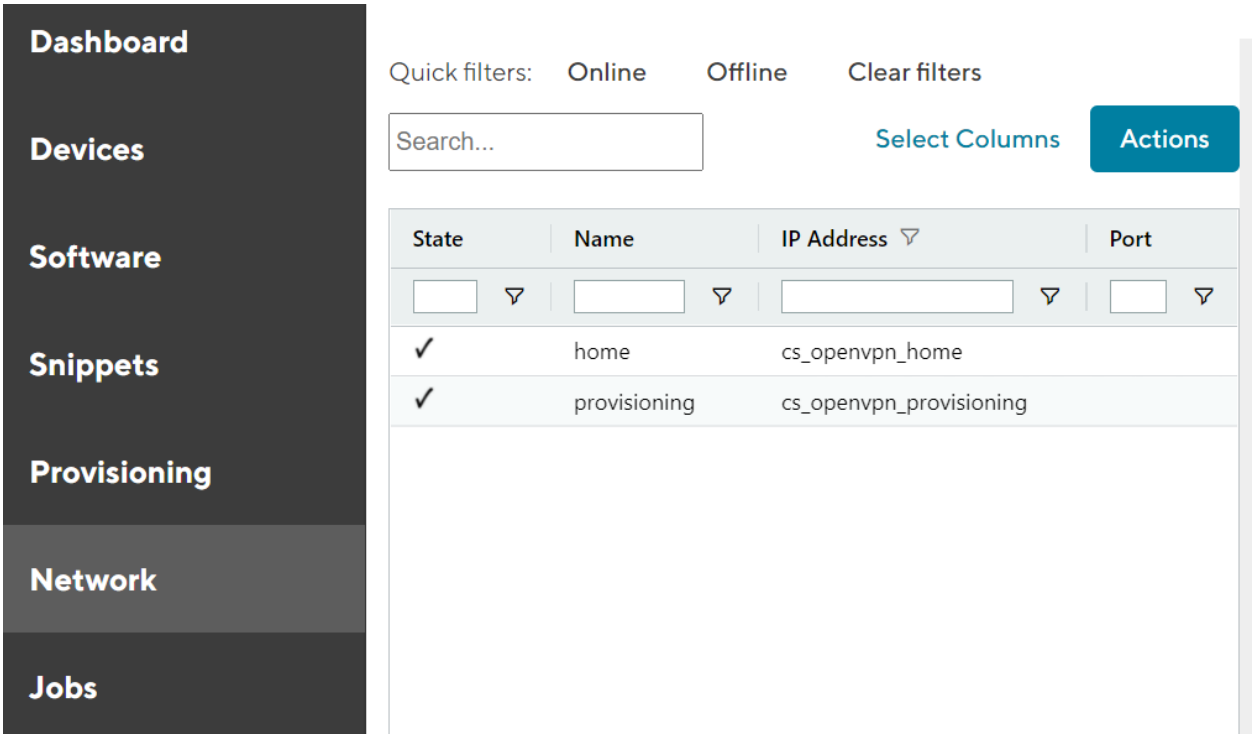

Fig. 4.1: Network overview

4.3.1 Configure the Tenant types

Between one, two or three Tenants type can be chosen depending on the layout for the Home Network (see Section 7 for more detailed explanation of the network architecture).

1. To add a Tenant, navigate to the "Network" page of the Connectivity Suite UI. Click on "Actions" at the upper right corner of the Main dialogue box and Click "Add Tenant".
2. Fill out the required fields and click "Add Tenant" to start the assignment of a Tenant. A confirmation message must pop up which confirms the assignment of the Tenant.
3. The Tenant will now be listed in the table in the Main dialogue box. When the status shows a green tick, the Tenant is ready for use. It can take up to two minutes until the Tenant shows up in the table (see Fig. 4.3).

Tenant Details OpenVPN Network

Shortname	Name of the Tenant
IP Address in Home Network	IP address which is assigned to the tenant by the home server.
Tenant Network	Subnet of the tenant in the home network
Network behind NAT	The internal network address of the Tenant The internal network is a subnet of the Home network changed by NAT (see Section 7 for more detailed explanation).
Port	The UDP port number of the server where the Connectivity Suite is running (needs to be open in the firewall to connect Devices to the Tenant).

Tenant Details Routers and End Devices

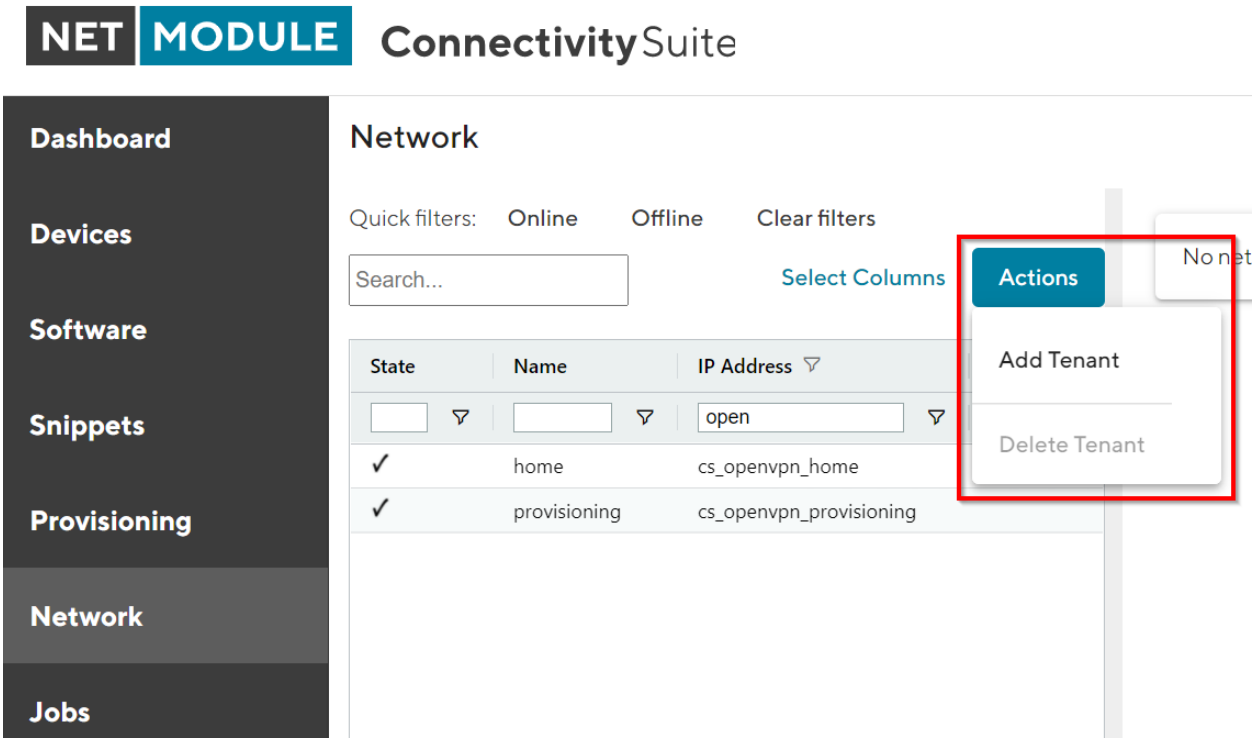

Fig. 4.2: Add Tenant

Tenant Type	Defines the max. number of possible Tenants which can be added and max. number of Devices which can be connected to the Tenant. The Tenant type has been defined already during the installation of the Connectivity Suite and cannot be changed anymore (see Section 7.1 for more detailed explanation).
Max. number of routers	The maximum numbers of routers which can be connected to the Tenant.
Number of routers left	The number of routers that can be added to the tenant (see Section 7 for more detailed explanation).
End devices per router	The number of End Devices that can be connected to the tenant.

The procedure is required for every single Tenant. The default values can be overwritten when new Tenants are created in the Connectivity Suite, i.e. these properties can be set per Tenant.

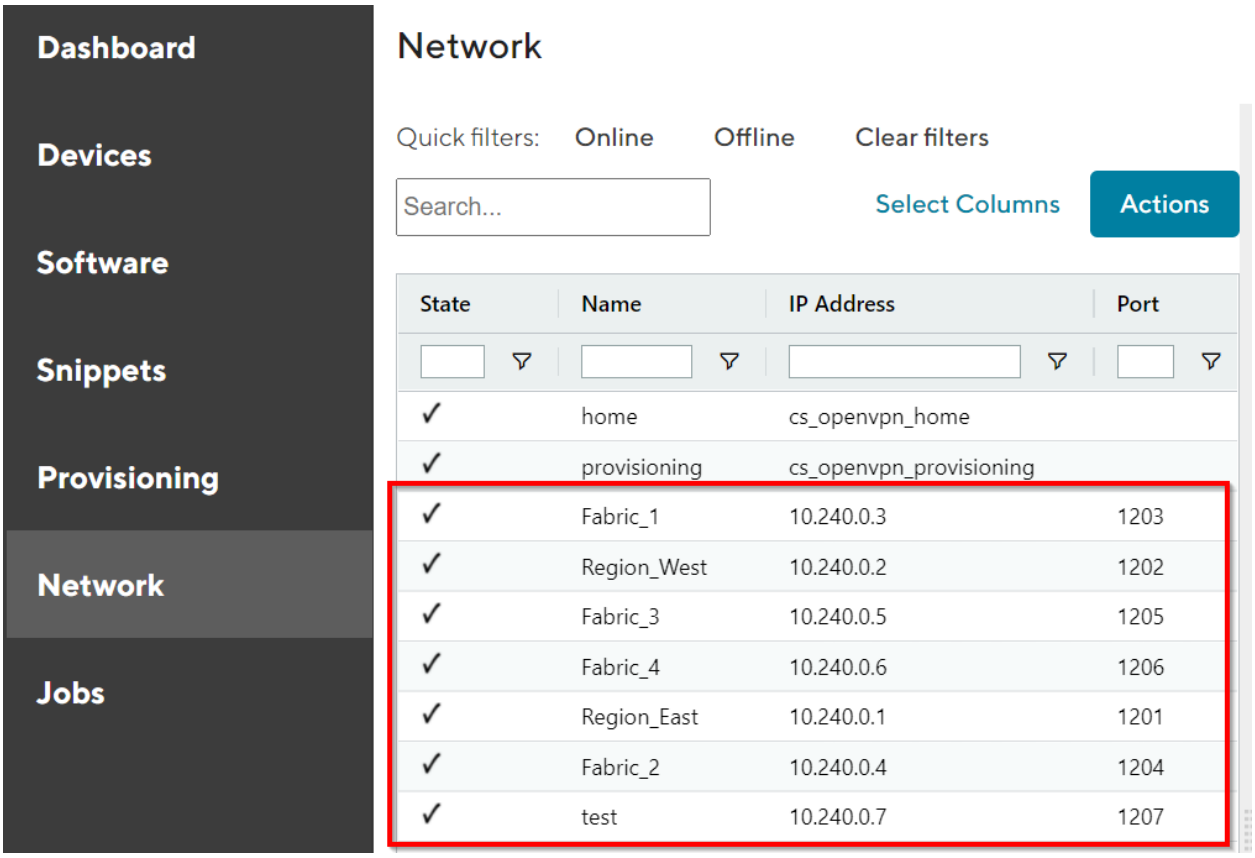

Fig. 4.3: Tenant added

4.3.2 Adding remote Tenant

Warning: Remote Tenants are recommended when you intend to connect more than 250 devices to the Connectivity Suite. This ensures an efficient operation.

1. To add a Tenant, navigate to the "Network" page of the Connectivity Suite UI. Click on "Actions" at the upper right corner of the Main dialogue box and Click "Add Tenant".
2. Fill out the required fields including the field "Remote Tenant" and add the domain name or IP address of the remote tenant machine, than click "Add Tenant" to start the assignment of a Tenant.

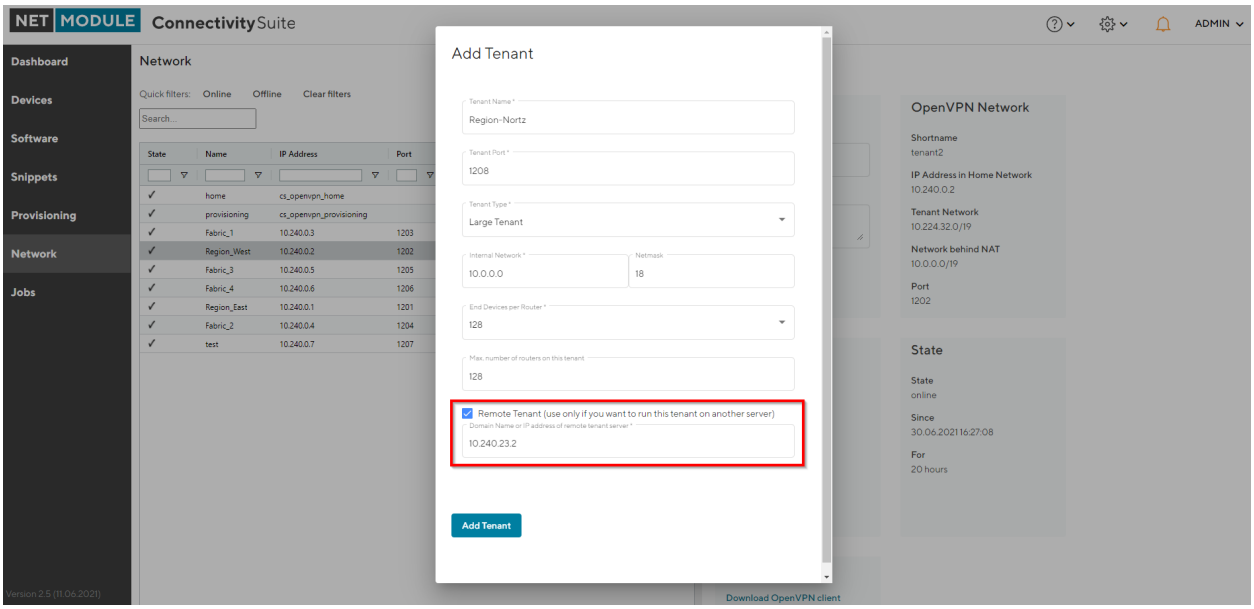

Fig. 4.4: Add Remote Tenant

3. Download the remote tenant installer package (this can either be done directly from the pop-up displayed right after the tenant creation or later via the Network page by clicking on the download symbol under Remote Tenant Installer next to the respective tenant (see Fig. 4.5).
4. After downloading the installer package, follow the instructions given in the README.txt which is included in the package.

4.4 Adding Routers to the Connectivity Suite

4.4.1 Supported NM router firmware releases

Before adding a router to the Connectivity Suite ensure that a supported firmware is running on the device. The Connectivity Supports the actual supported router firmware.

Note: The Connectivity Suite guarantees support for all active NM router firmware releases. These can be checked at the following link: https://wiki.netmodule.com/documentation/releases?s{[]{[]}=nrsw

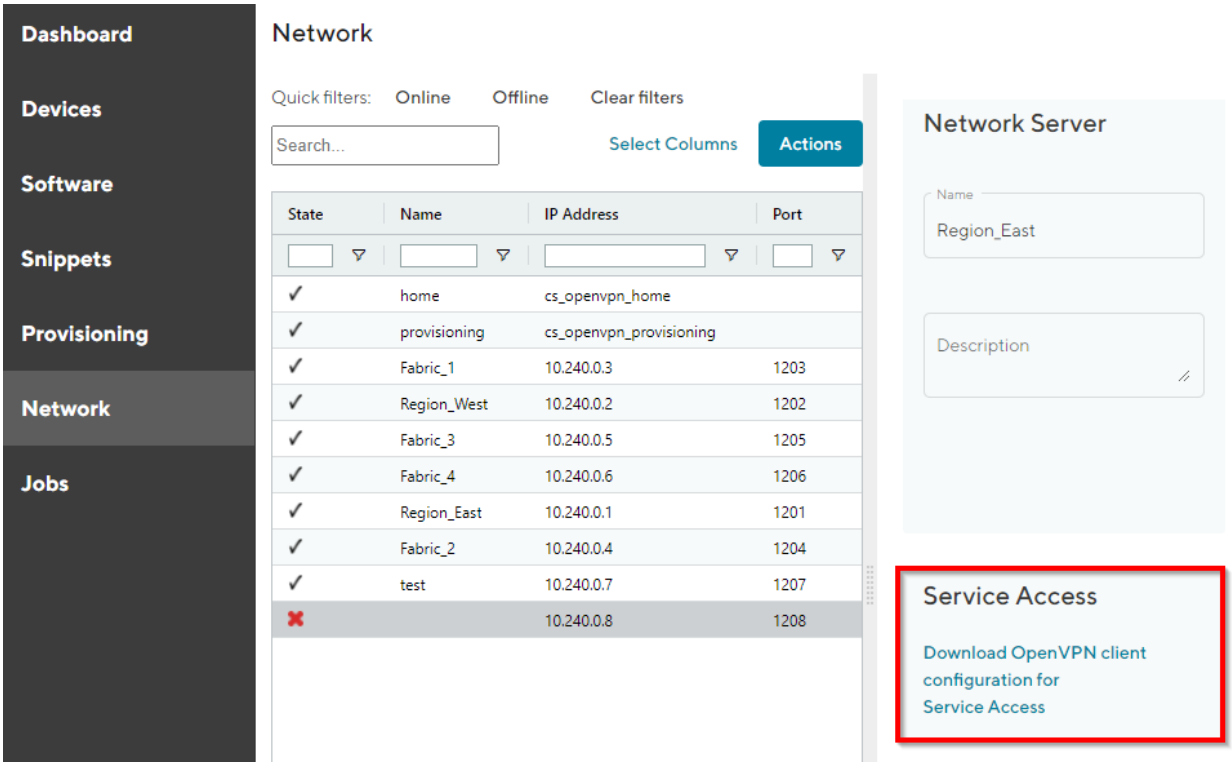

Fig. 4.5: Download Remote Tenant

Older releases can also work with the Connectivity Suite, but it is recommended to update to the latest firmware as soon as possible, as support is not guaranteed for these releases.

4.4.2 Initial router provisioning

To add Devices to the Connectivity Suite they require an initial provisioning to ensure an automatic assignment of the Device to the Connectivity Suite. In this process the Provisioning Configuration for your Device is created which enables the Device to access to the Connectivity Suite. When a Device has been supplied with this configuration it automatically connects to the Provisioning Server of the Connectivity Suite via a VPN connection, the Device can than be administrated through the Connectivity Suite. The next step after the provisioning is moving the Device to a Tenant (see Section 4.5). This must be done to enable all Connectivity Suite features for a Device.

Warning: Only 250 devices can be connected to the provisioning server at once. If the provisioning server has no available space left move the connected Devices to a Tenant before adding more.

For the following steps an account with **Platform Administrator** rights is required.

4.4.3 Create provisioning configuration

This chapter describes how to create the configuration required by the NM router to connect automatically to the Connectivity Suite for the first time.

Steps to be executed on the web interface of the router:

1. Only required if the router is in factory state: Go to the Web Manager of your NM router and set an administrator password.
2. Only required if the router is in factory state: Set the NM router to WAN mode and change the firewall settings accordingly.
3. Download the current configuration from the NM router via the web interface and make sure the device is connected to the internet. This file will be needed to upload it to the Connectivity Suite

Steps to be executed on the web interface of the Connectivity Suite:

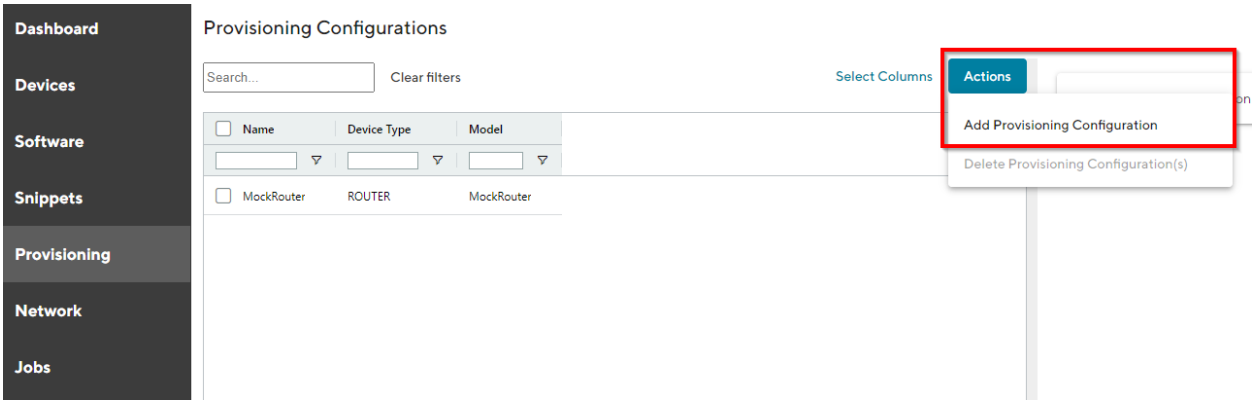

Fig. 4.6: Add Provisioning Configuration

1. For the initial NM router provisioning navigate to the page “Provisioning” on the Dashboard. Click on “Actions” at the upper right corner of the Main dialogue box and Click “Add Provisioning Configuration”.
2. Fill out the required fields and Import the configuration file that has been downloaded from the NM router by click on “Browse…”.
3. Click “Generate Provisioning Configuration” to upload the configuration to the Connectivity Suite. A confirmation message must pop up which confirms the upload of the configuration.

The uploaded configuration will be shown in the Main dialogue box in the table:

4.4.4 Add provisioning configuration the NM router

Warning: The configuration used to provision the router must originally be generated from the same router model. Example: it is not allowed to upload router configurations from a NB1600 and use this configuration to provision a NB800.

1. Select the required configuration in the Main dialogue box.
2. Click on “Download this configuration as USB version” in the lower right corner of the Detail dialogue box to download the provisioning configuration.
3. Unzip downloaded zip-file.

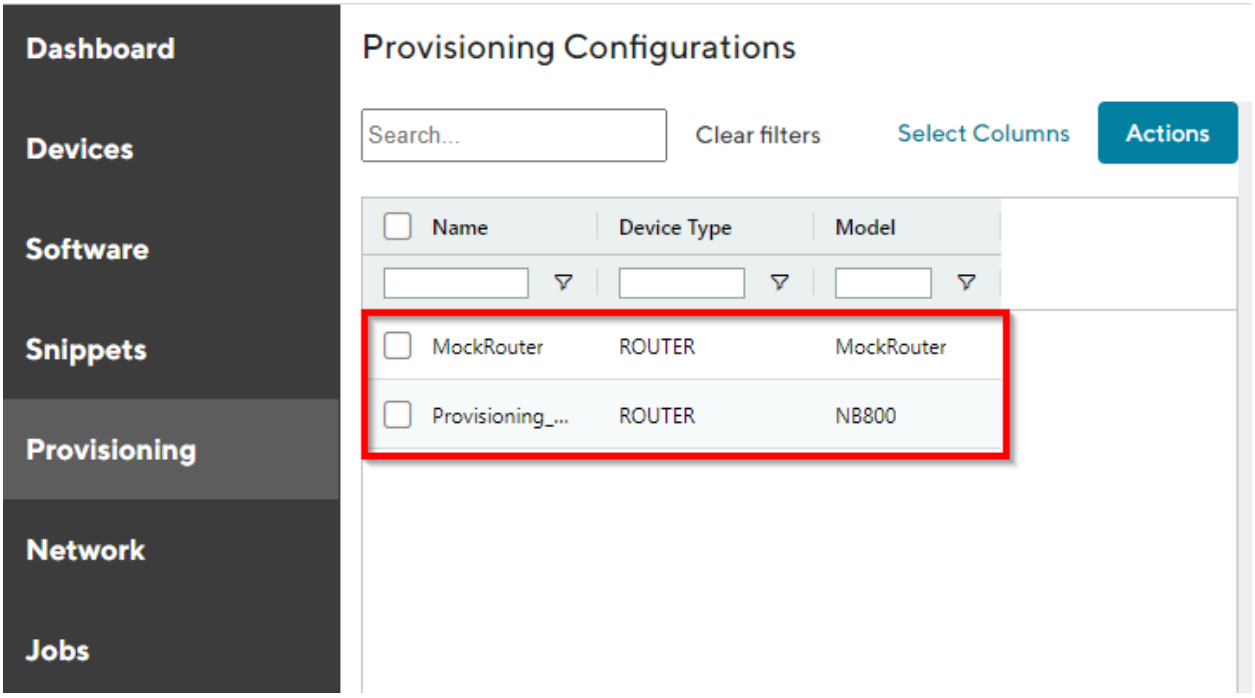

Fig. 4.7: Configuration table

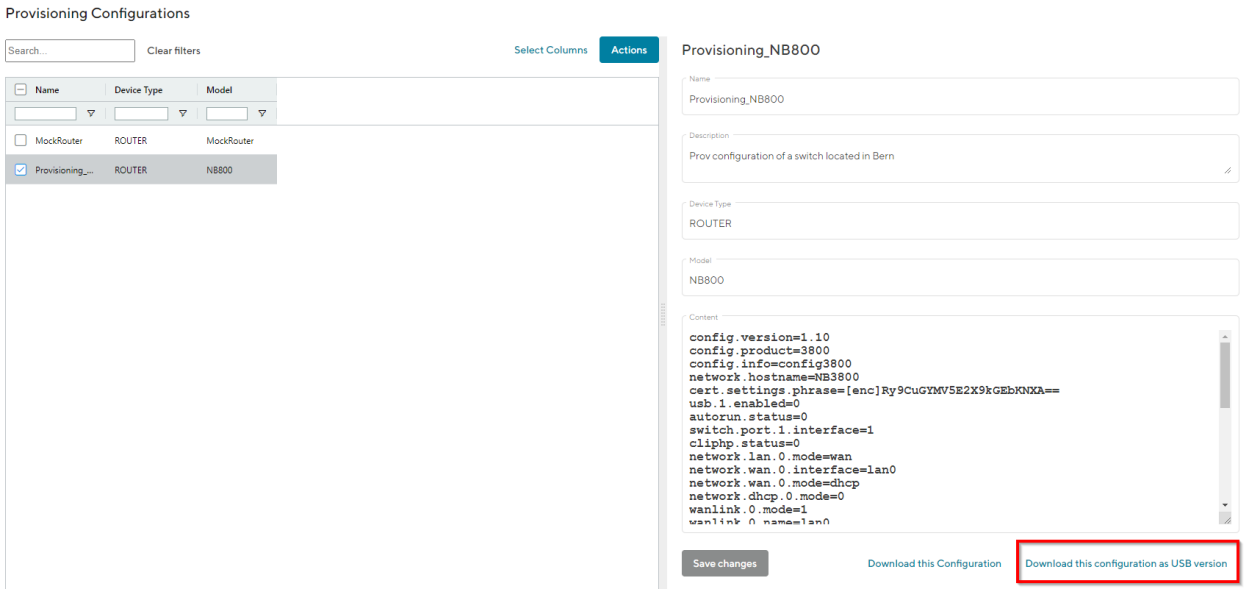

Fig. 4.8: Manual USB update

4. Copy the content of the extractet zip-file to an empty USB stick.

Warning: Do a factory reset of your NM router before uploading the configuration. This is necessary because the USB port has been disabled after your first login.

5. Plug the USB stick into your router to start the configuration update.
6. The router will now automatically apply the provisioning configuration and connect to the Connectivity Suite

As soon as all LEDs are blinking after connecting the USB stick, the USB stick can be removed.

Warning: The USB stick which is used to configure the NM router must be a FAT16/32 formatted USB stick.

4.4.5 Provisioning via the Web Manager

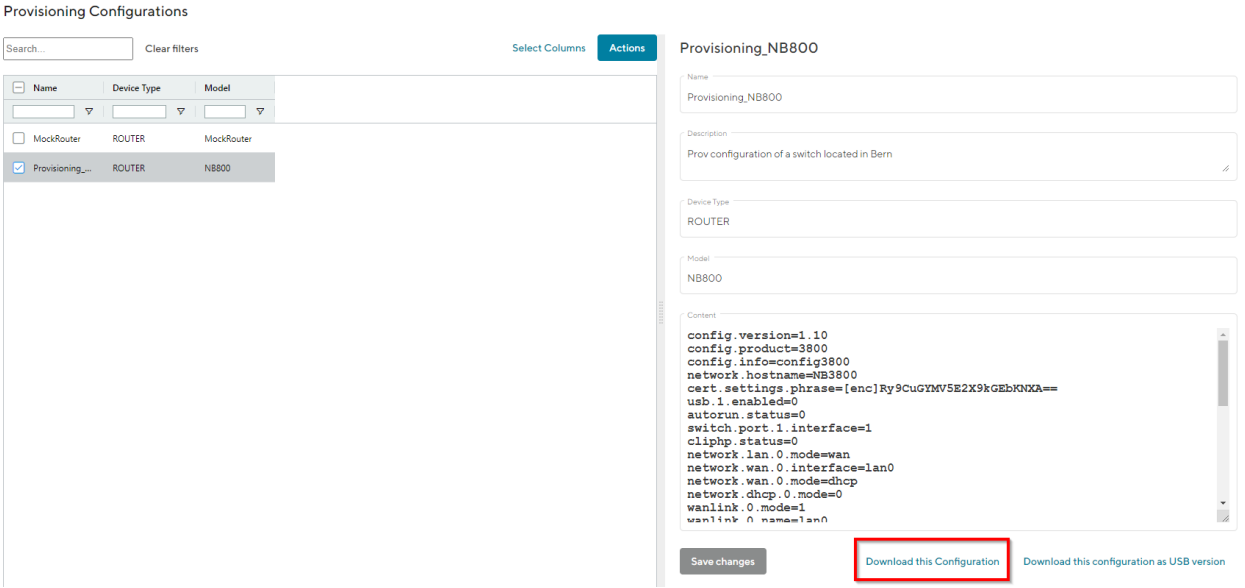

Fig. 4.9: Manuel file update

1. Click on “Download this Configuration” at the bottom of the Detail dialogue box to download the provisioning configuration.
2. Upload the file config.zip onto your NM router to start the configuration update. The configuration process starts.
3. The Device will now automatically connect to the Connectivity Suite.

4.4.6 Router connection check

To ensure that the Device has been connected navigate to the page “Devices” of the Connectivity Suite UI. Search for the serial number of the Device in the table of the Main dialogue box (The serial number of the Devices is automatically recognised and displayed by the Connectivity Suite). The row “state” in the table of the Main dialogue box shows whether the device has connected correctly to the Connectivity Suite. The Connectivity Suite detects to states:

tick state: The tick indicates that a Device is pingable from the Connectivity Suite Home Network. It does not indicate that all functions of the Device are working correctly.

cross state: The red cross state indicates that a Device is not pingable from the Connectivity Suite Home Network.

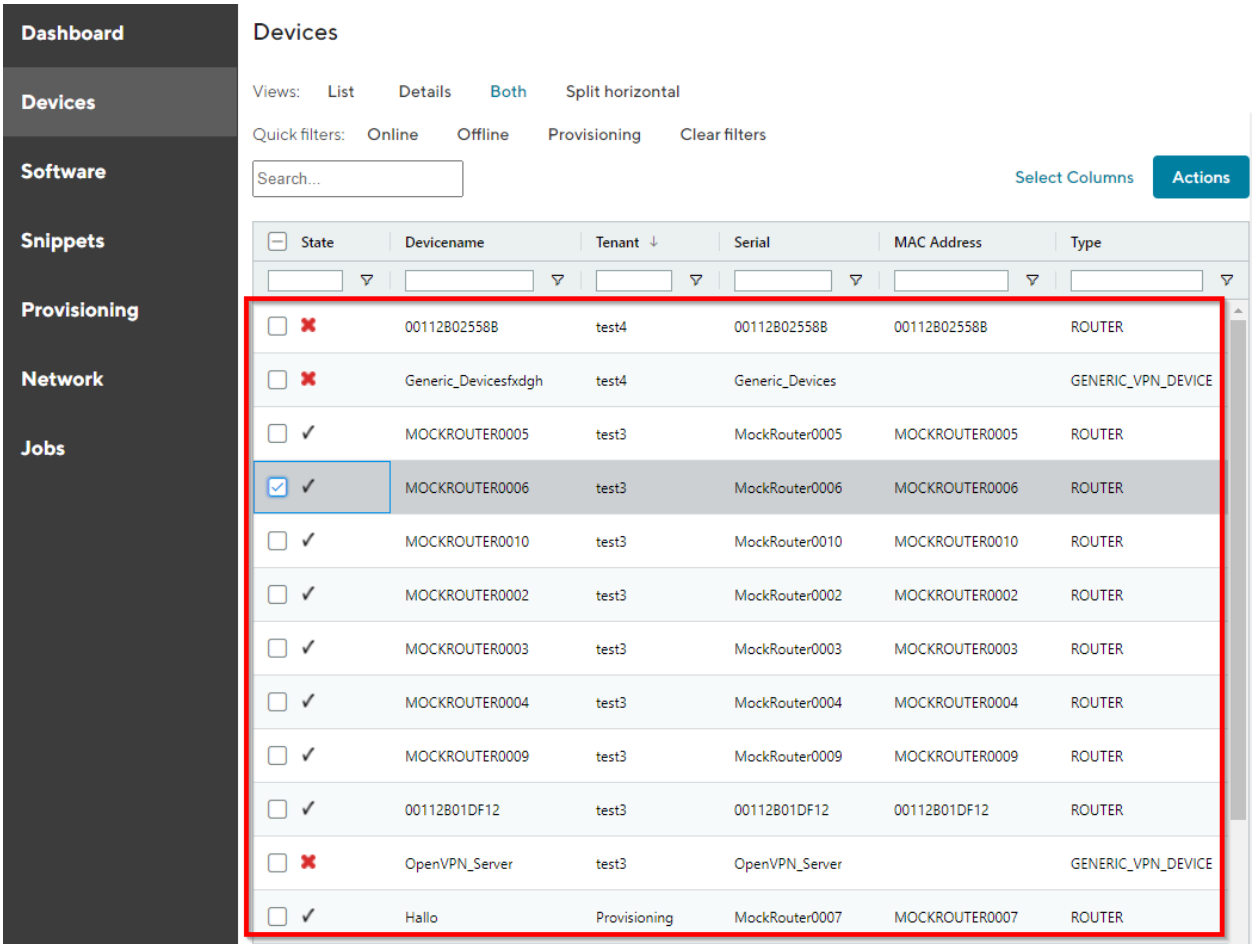

Fig. 4.10: Device overview

4.4.7 Router status check

If the device has connected correctly you can see all the Device details by clicking on the device in the table of the Main dialogue box. In the tab “Device Details” several status information about the selected Device is listed (see Fig. 4.11).

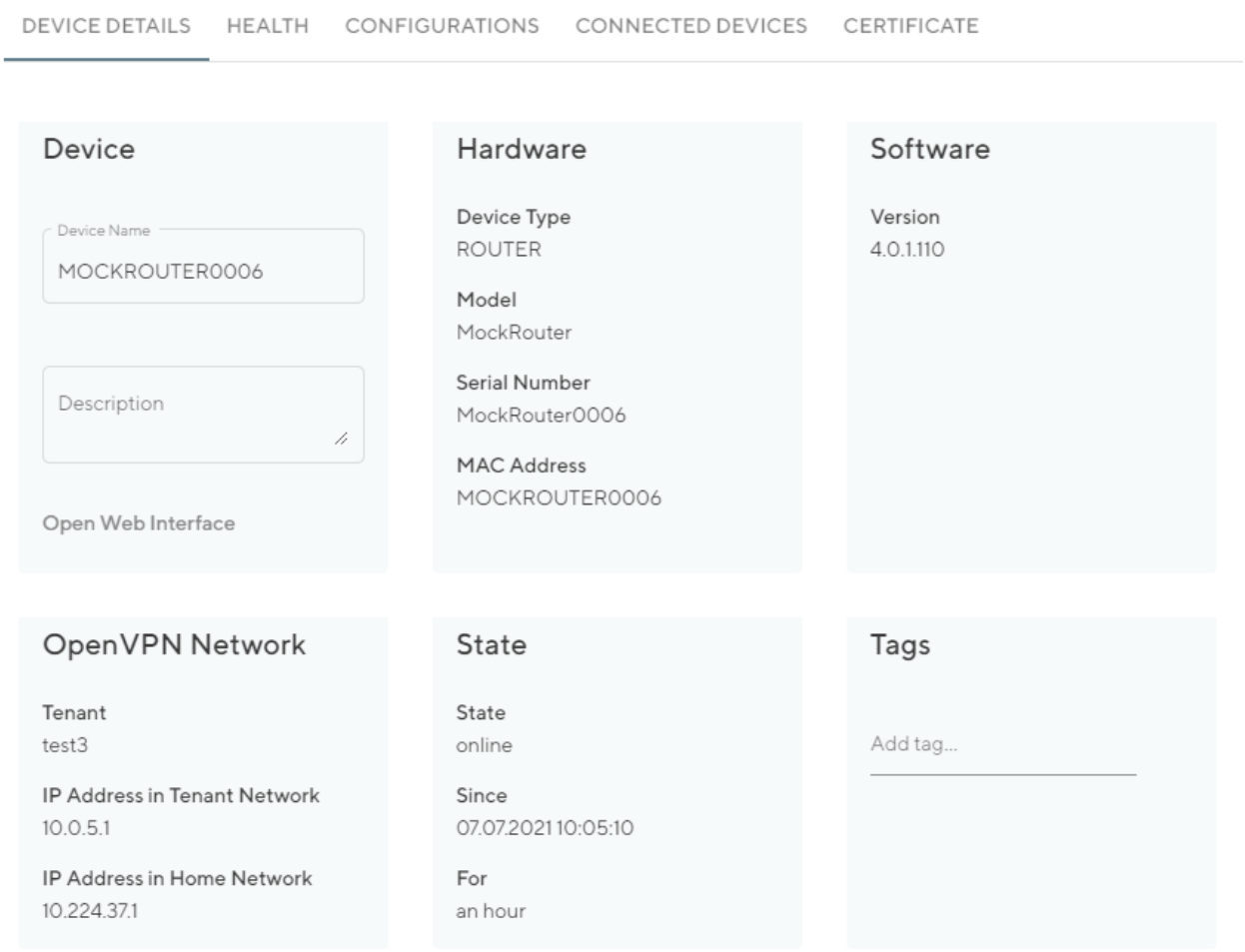

Fig. 4.11: Device Details overview

Device	The name and description of the Device are displayed which can be customised by the user
Hardware	Device-specific information is displayed here which cannot be changed.
Software	Shows the software version which is running on the Device
OpenVPN Network	Shows the IP addresses of the Devices
State	Shows the status of the device connection with the Connectivity Suite
Tags	User-specific tags for further designations of devices

Health: In the tab “Health” the connection status of the Device is displayed. The Connectivity Suite periodically pings whether the device is connected. If the connection is interrupted, the device switches from online to offline status.

Configurations: In the tab “Configuration” the actual Configuration is displayed incl. the name of the Configuration. It is also possible to modify, download or retrieve the Configuration from the Device via this tab.

Connected Devices: In the tab "Connected Devices" all End Devices are displayed which are connected to the selected Device.

Certificate: In the tab "Certificate" the validity duration of the actual valid certificate is shown. This certificate can be renewed or revoked. If the certificate is revoked the Device will lose the connection. Connectivity Suite Quick User Guide 25/48

4.5 Adding a Device to a Tenant

4.5.1 (Initial) Tenant assignment of a Device

> **Warning:** It is recommended to connect maximum 250 devices to a Tenant to ensure an efficient operation.

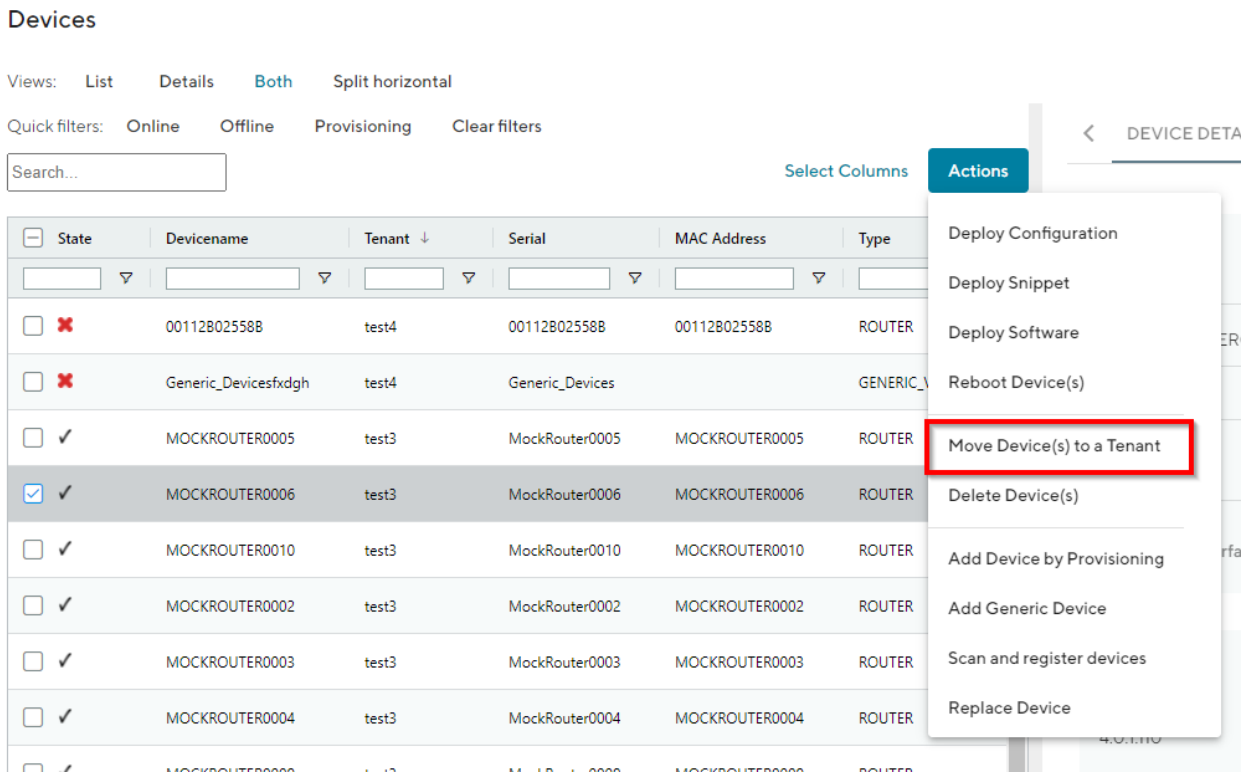

Fig. 4.12: Tenant assignment

1. Navigate to the page "Devices" of the Connectivity Suite and select the Devices which have to be assigned to a Tenant.
2. Click on "Actions" at the upper right corner of the Main dialogue box and click "Move Device(s) to a Tenant".
3. Select the required Tenant in the drop down list and click "Next".
4. Click on "Start assignment" to assign the Devices to the Tenant (this operation may take some time). A confirmation message must be pop up which confirms the assignment of the Devices to the Tenant.
5. The applied Tenant will be shown in the Main dialogue box in the table.

4.6 Connect Networks with identical IP address ranges

The Connectivity Suite provides the function to connect networks which have identical IP addresses within their subnet. This function is enabled by 1-to-1 NAT. As example all Devices within a Tenant can have the same IP-configuration.

4.6.1 1-to-1 NAT on Tenants

While creating a new Tenant, an internal network must be provided for this Tenant. This network consists of all the Devices assigned to this Tenant, plus possible other VPN clients, like Service Access users or backend servers. Note that the same network address range can be used on multiple Tenants. The Tenants do a 1-to-1 NAT mapping, thus allowing the Connectivity Suite to individually address any Device on any Tenant (see Fig. 12.1).

4.6.2 1-to-1 NAT on NM Routers

The concept mentioned in Section 4.6.2 also applies to the NM routers, so that multiple routers can have the same internal network address range, while the Connectivity Suite is still able to individually address any End Device behind any router (see Fig. 12.1). Therefore 1-to-1 NAT must be configured on the NM routers.

CHAPTER

FIVE

DEVICE MANAGEMENT

5.1 Dashboard

The Dashboard provides full summarized overview of the status of the network infrastructure. In the field Devices all Devices are shown which are online, offline or in provisioning state. The Jobs field provides the status about the Jobs to be executed (see Section 5.4.1). The Network Servers field shows how many networks (Tenants) are setup and online.

5.2 NM router configuration update

The CS can roll out configuration updates to Devices. The main feature here is mass configurations that can be rolled out for different types of Devices. In addition, configurations of individual devices can also be copied or adapted via the CS.

Note: For the following steps an account with Platform or Tenant Administrator rights is required. A Platform Administrator can execute Configuration updates cross-Tenant whereas a Tenant Administrator can only update Devices of his Tenants.

5.2.1 Mass configuration updates

To execute mass configurations, the Connectivity Suite uses so-called snippets. A snippet is an excerpt from the configuration parameters that configures a specific function of the router, e.g. activating the USB port or switching off WLAN. Snippets can be used to configure an infinite number of Devices, regardless of the Device type (only applies to NM devices).

All configuration parameters which can be used for a Snippet are documented and can be found in the NM Wiki using following link: https://wiki.netmodule.com/documentation/config-parameters?s{[}{]}=parameter

Example of a complete Snippet that originates from a configuration with version 1.8 and enables the USB port 0:

```
config.version=1.8
usb.status=1
usb.0.enabled=1
```

Before the configuration can be deployed for a massconfiguration a Snippet must be created:

1. Navigate to the page “Snippets” and click on “Actions” and “Add Snippet” to add a snippet.
2. Fill out the required fields and click “Add Snippet” to save the Snippet.

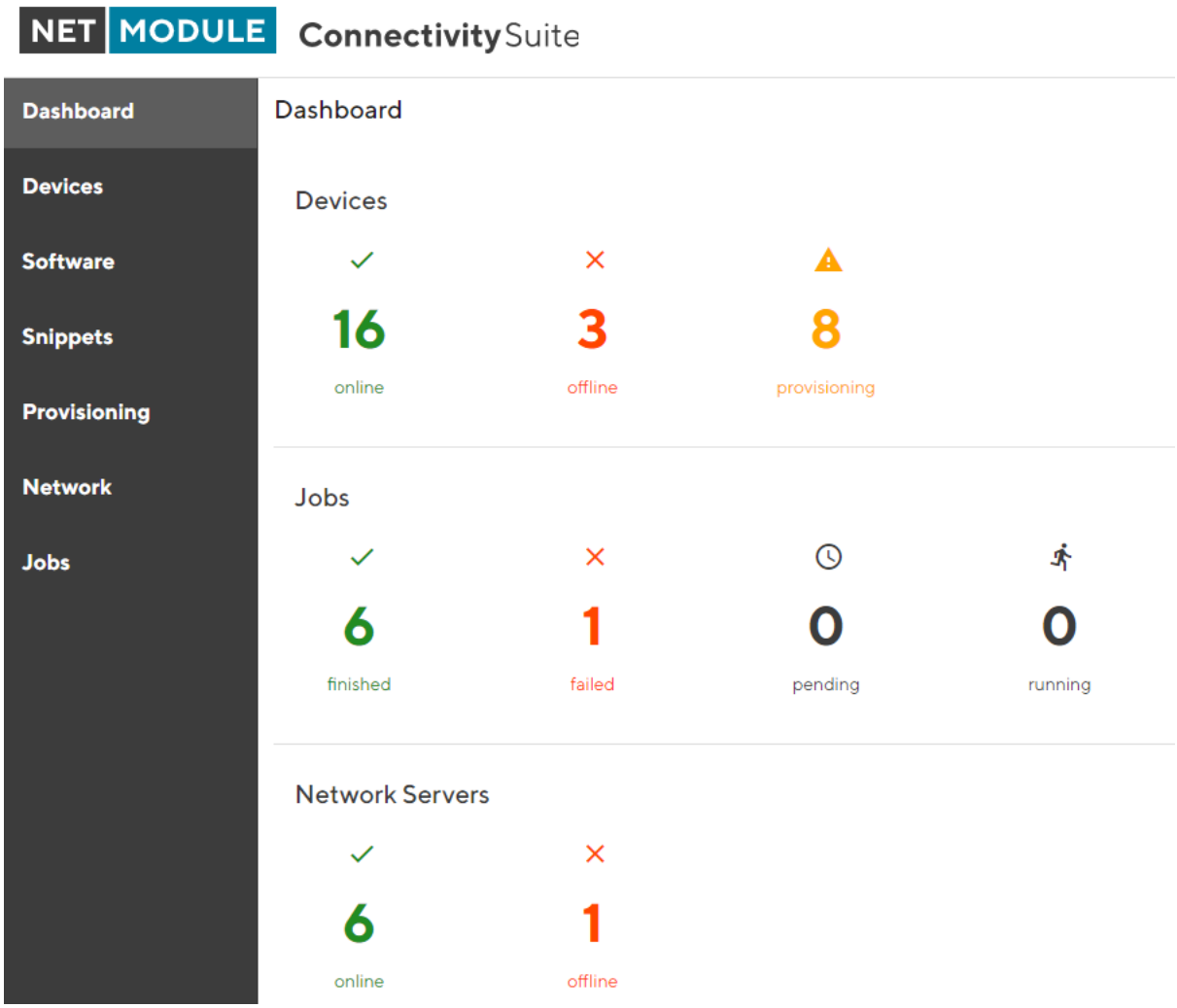

Fig. 5.1: Dashboard

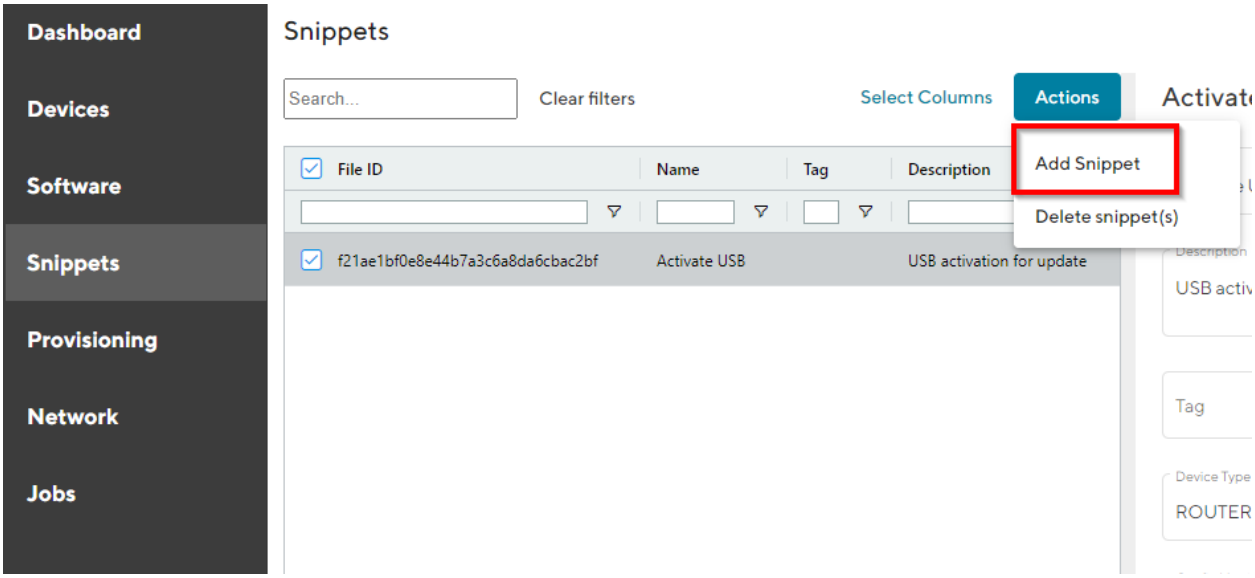

Fig. 5.2: Add Snippet

When creating the Snippet following parameters can be set:

Name	Name of the Snippet
Description	Description of the Snippet to be executed
Tag	Tag to identify the Snippet
Device Typ	Device type can be a NM switch or router
Config Version	Describes the version of the configuration parameters used in the Connectivity Suite. The configuration version is forwarded to the routers. Routers that use an older or newer version can now adjust the configuration parameters accordingly. You will find the configuration version in the first line of a every router configuration (see Fig. 5.3).
Content	Subset of configuration parameters taken from a user-config.cfg file can be filled in this field

3. A confirmation message will pop up. The added Snippet will be listed in the Main dialogue box in the table.
4. Once the Snippet is available in the Connectivity Suite you can update one or several Devices with the same Snippet. Navigate to the page “Snippets” and select the Devices in the main dialogue Box that are to be configured.
5. Click on “Actions” at the upper right corner of the Main dialogue box and click “Deploy Snippet”.
6. Select the Snippet to be deployed.
7. Select whether you want to start the configuration immediately or whether it should be scheduled.
8. Confirm the deployment by click “Start deployment”.

When a Snippet deployment has started it will be listed as a Job in the Jobs table (see Section 5.4). Jobs can be scheduled while creating them (see step 7). Therefore following scheduling options are possible:

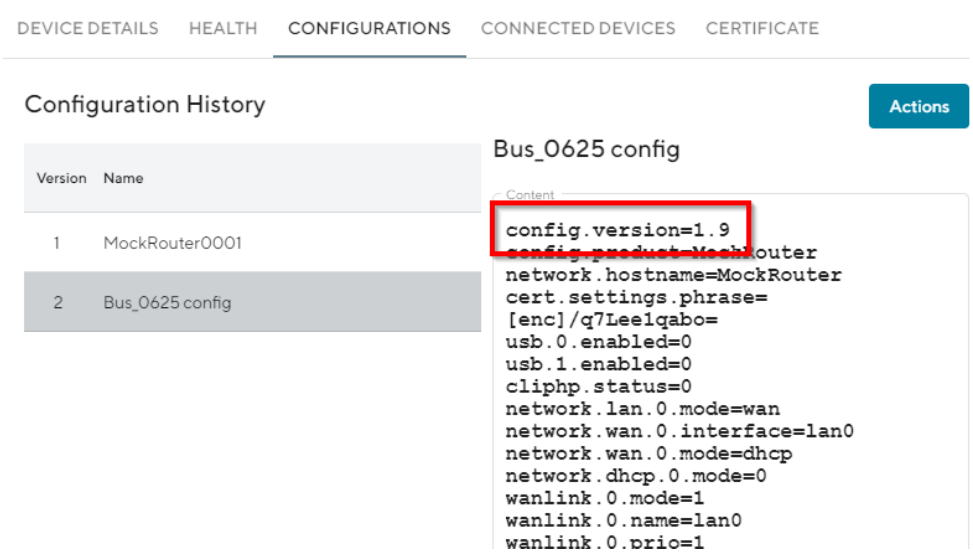

Fig. 5.3: Configuration version

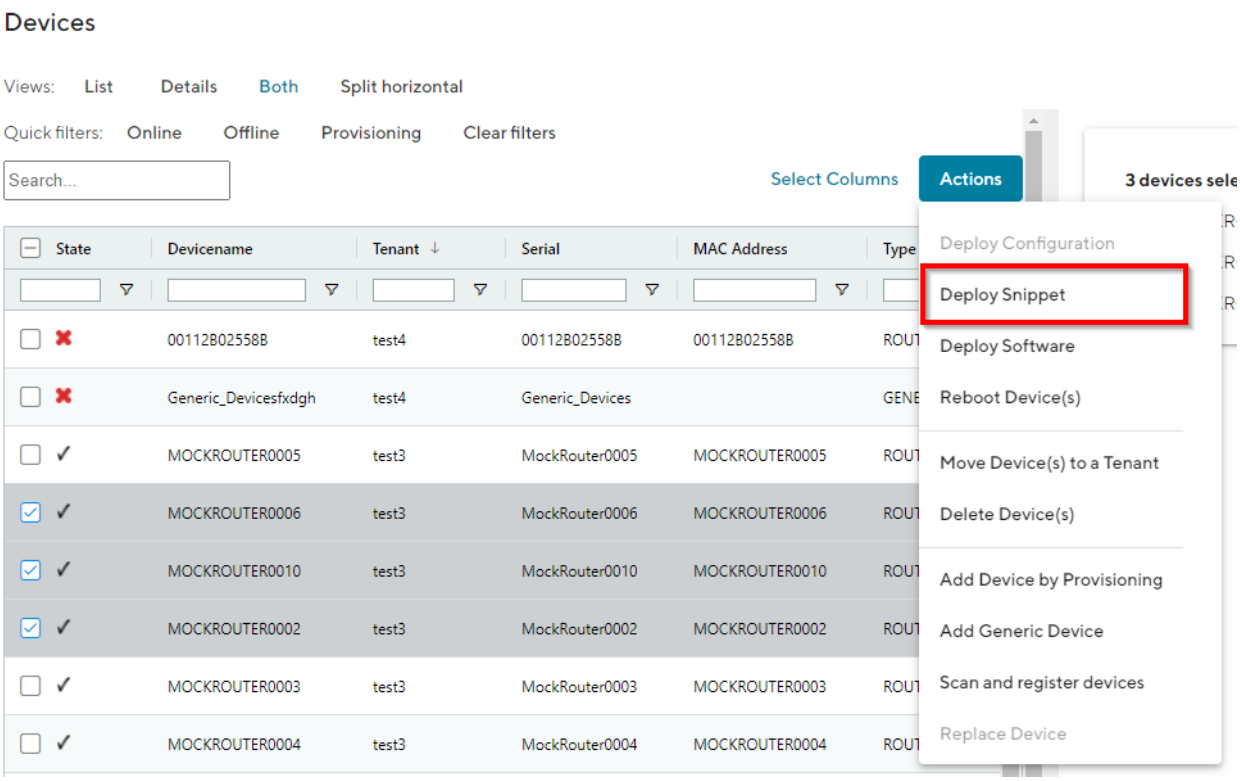

Fig. 5.4: Configuration update

Start Date	The first day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.).
End Date	The last day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.).
Days	Offers the possibility to constrain the execution of the Job to specific days of the week. By default, the execution is allowed for all days of the week (the blue color indicates a selected day)
Start Time	Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 0-23, the default value is 0 (midnight).
End Time	Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 1-24, the default value is 24 (midnight).

Warning: Configuration changes made in the web interface of the Device will not be automatically added to the Connectivity Suite and can lead to connectivity issues. Any configuration changes made in the web interface of a NM router must be uploaded to the Connectivity Suite as described in Section 5.2.4.

5.2.2 Copy Device configurations

Using the Connectivity Suite, configurations can be copied from one Device to another Device of the same type. To copy configurations across devices, follow the instructions below:

1. Navigate to the page "Devices" of the Connectivity Suite and select the Device in the table of the Main dialogue box from which the configuration is to be copied.
2. Click on "Actions" at the upper right corner of the Main dialogue box and click "Download this configuration" (configuration can be uploaded via the web manager) or "Download this Configuration as USB version" Configuration can be uploaded via an usb stick).
3. Select the Device in the table of the Main dialogue box to which the downloaded configuration is to be copied.
4. Click on "Actions" at the upper right corner of the Main dialogue box and click "Upload configuration".
5. Select the downloaded configuration from step 2 and click "Uploade Device Configuration"
6. Click on "Actions" at the upper right corner of the Main dialogue box and click "Deploy Configuration".
7. Select the configuration version to be deployed from step 5.
8. Select whether you want to start the configuration immediately or whether it should be scheduled.
9. Confirm the deployment by click "Start deployment". The job can be started (b) immediately or (a) scheduled.

5.2.3 Restore configuration

Each time a standard configuration is changed, a new configuration version is created rather than overwriting the current configuration. This way, a history of all previous configurations for each Device is recorded. Therefore, The Connectivity Suite can reset a NM router to a previous state by deploying a specific configuration version to it. The different configuration versions can be seen on the page "Devices" in the Detail dialogue box in the tab "Configurations".

The Connectivity Suite creates a configuration version when following happens:

- If a Device connects for the first time with the Connectivity suite

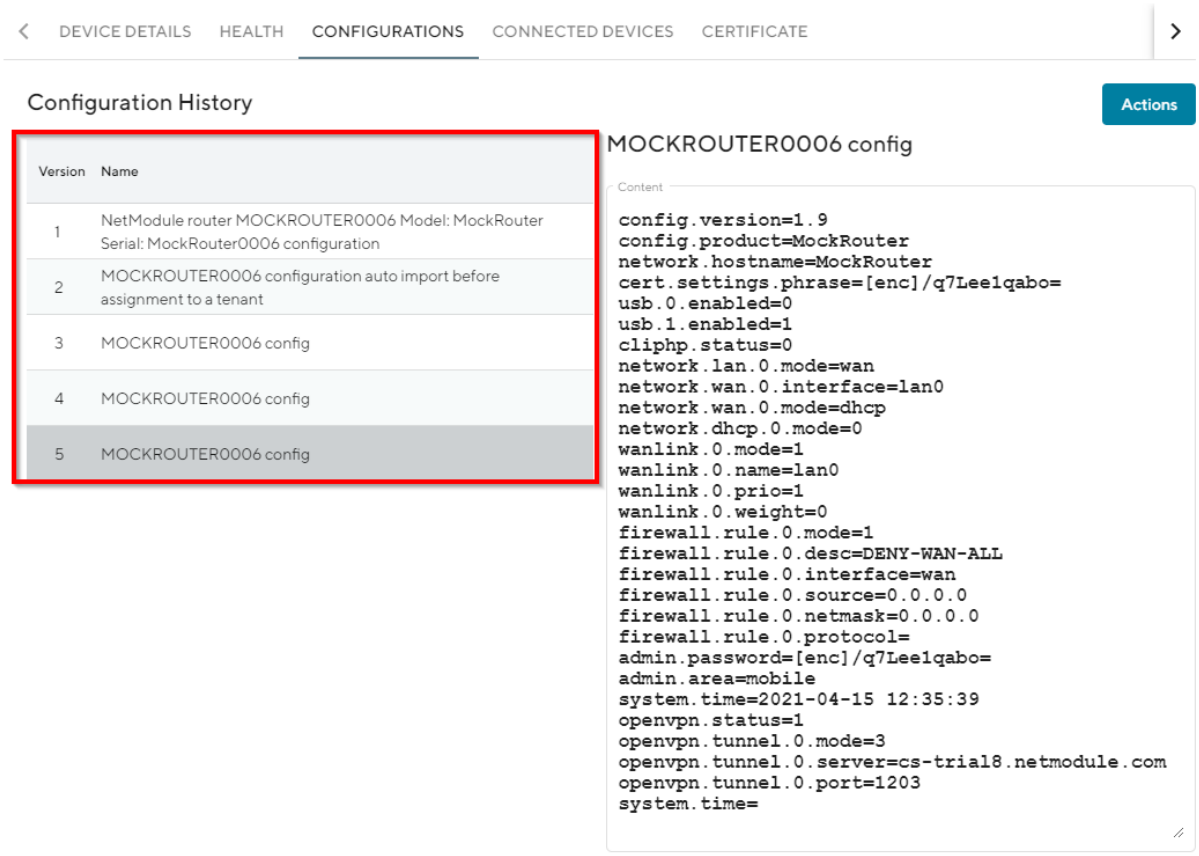

Fig. 5.5: Configuration versioning

- If the Connectivity Suite has executed a configuration update
- When a Device is moved to a tenant
- Before the Connectivity Suite performs a configuration update (backup copy)

If you want to restore an old configuration follow the following steps:

1. Navigate to the page “Devices” of the Connectivity Suite and Select the Device on which an old configuration is to be restored.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Deploy Configuration”.

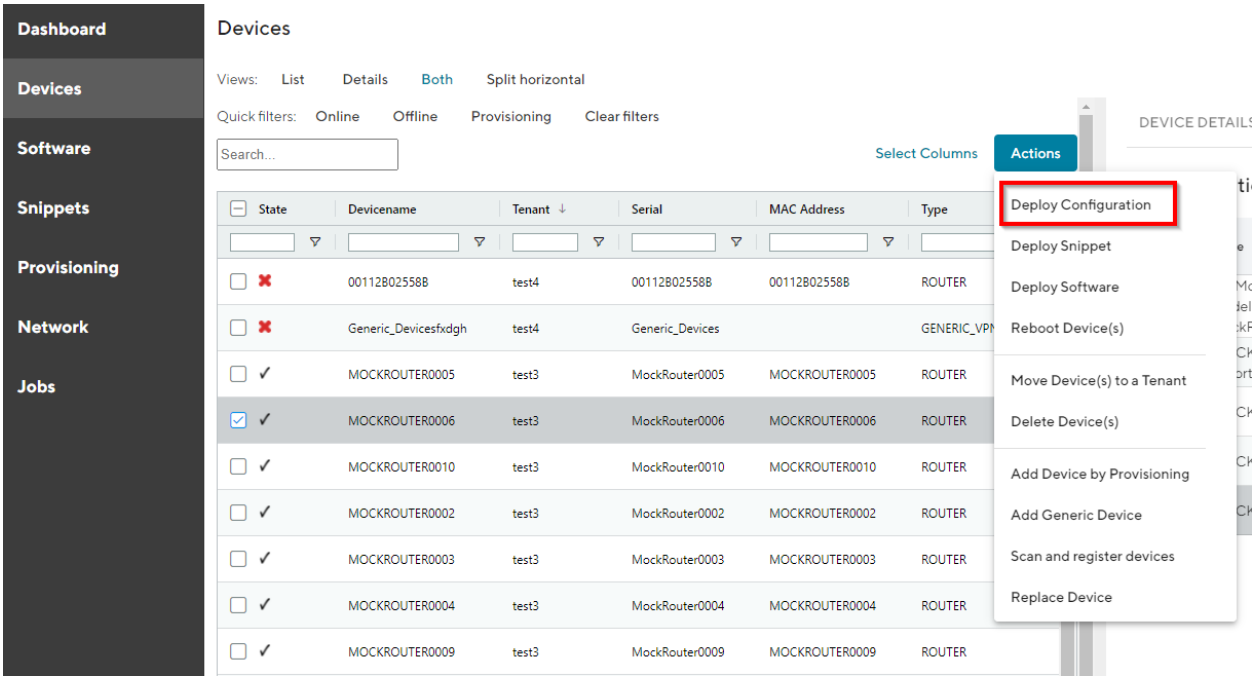

Fig. 5.6: Configuration restore

3. A list of all configuration versions of the Device is displayed. Select the configuration version to be restored.
4. Select whether you want to start the configuration immediately or whether it should be scheduled.
5. Confirm the deployment by click “Start deployment”.

5.2.4 Manual configuration updates

There are a few cases where the Connectivity Suite does not become aware of a Device configuration change, hence the current Configuration stored in the Connectivity Suite does not correspond to the one running on the Device and must be manually updated:

- if the change was made outside of the Connectivity Suite (e.g. via the web interface of a NM router or the router CLI)
- if an older configuration version has been deployed

In those cases, the user must manually trigger the import of the updated configuration to the Connectivity Suite.

1. Navigate to the page “Devices” and select in the Main dialogue the Device for which the configuration has changed

2. Open the tab “Configurations”, click on “Actions” at the upper right corner of the Detail dialogue box and click “Retrieve current configuraton from device”.

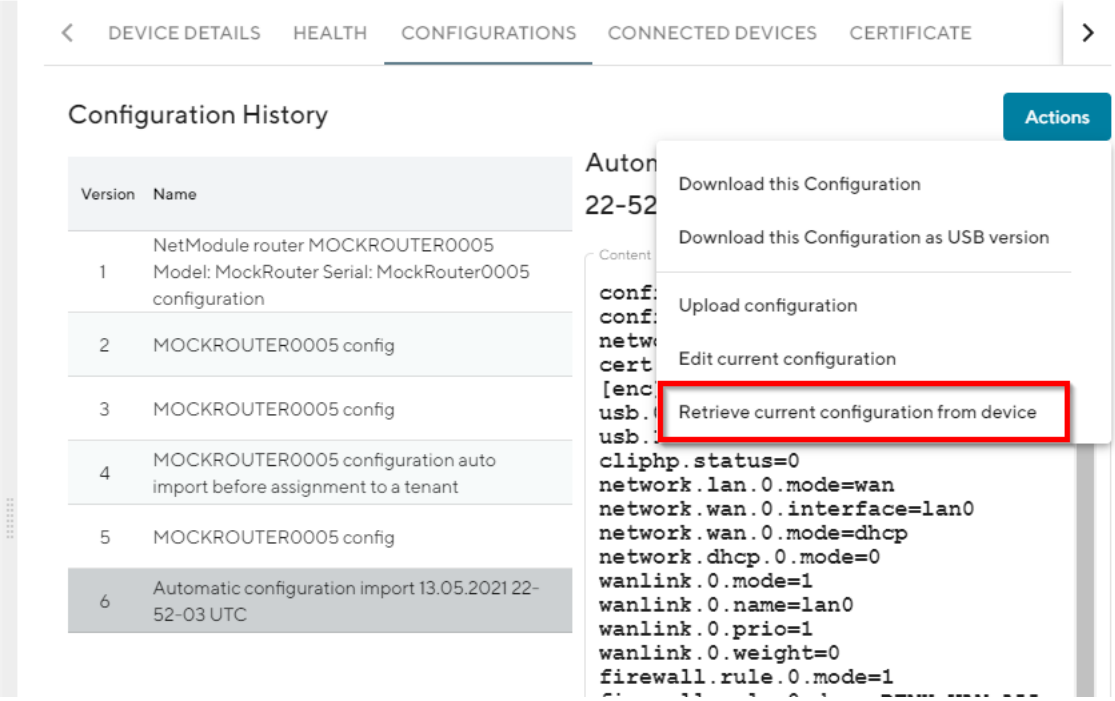

Fig. 5.7: Retrieve user configuration

3. Choose “Import current device configuration into Connectivity Suite” in the pop-up window. The configuration is now listed in the configuration history table.

5.3 Router software update

Whenever a software update for one or more Devices is required it can be executed via the Connectivity Suite. To get the latest software for your router go to http://netmodule.com/support/downloads.html and download it from the webpage.

Note: For the following steps an account with Platform or Tenant Administrator rights is required. A Platform Administrator can execute software updates cross-Tenant whereas a Tenant Administrator can only update Devices of his Tenant.

5.3.1 Upload Software to the Connectivity Suite

To execute a Software update, it is required to upload the Software first to the Connectivity Suite before executing the update. To add Software to the Connectivity Suite, follows the instructions below:

1. Navigate to the page “Software” and click on “Actions” and “Add Software” to add a Software.

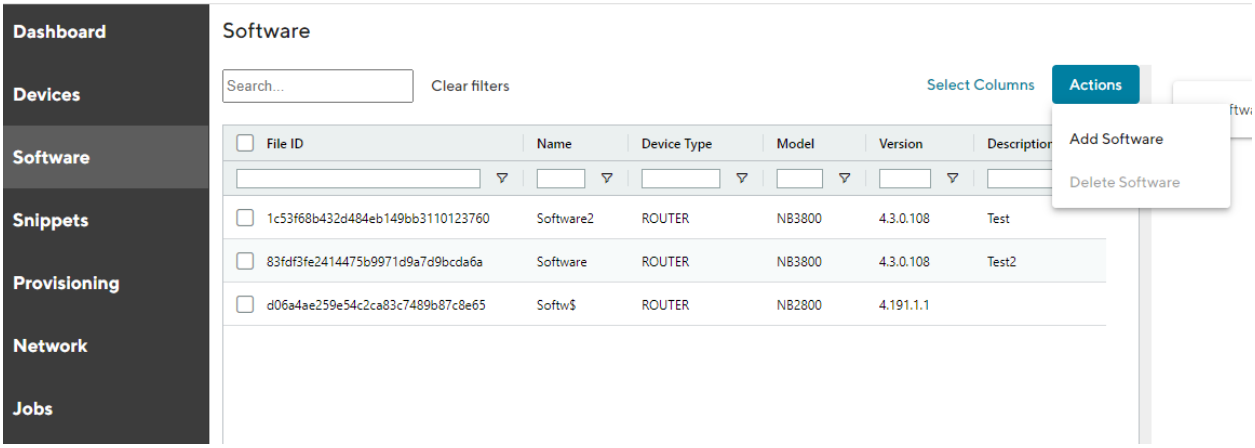

Fig. 5.8: Add software

2. Fill out the required fields and click “Add Software” to save the Software.
3. A confirmation message will pop up. The added Snippet will be listed in the Main dialogue box in the table.

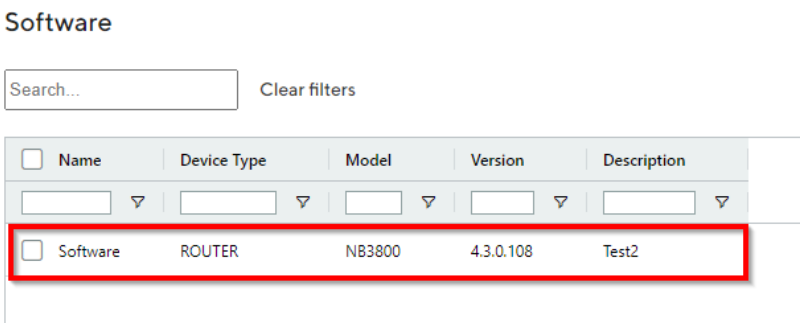

Fig. 5.9: Upload software

Note: It can take several seconds until the software has been uploaded.

5.3.2 Upload Software to the NM router

Once the Software is available in the Connectivity Suite you can update one or several Devices with the same Software image. The Job scheduling system allows you to schedule when a Software update is deployed.

1. Navigate to the page “Devices” and click on “Actions” and “Deploy Software” to upload a Software.

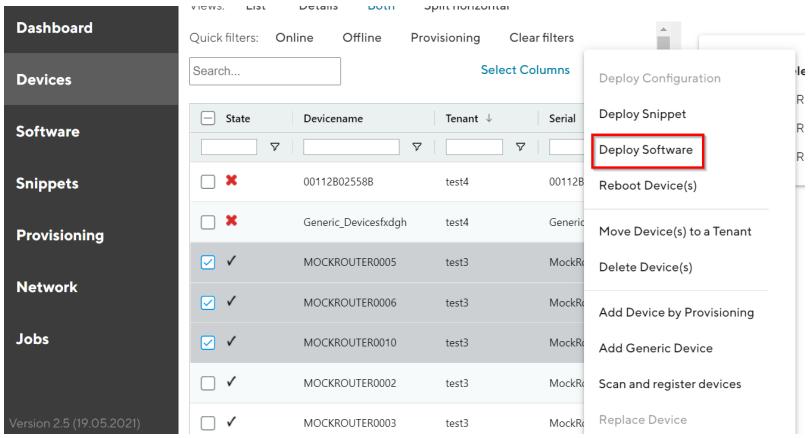

Fig. 5.10: Update Device software

2. Select the Software to be deployed.
3. Select whether you want to start the update immediately or whether it should be scheduled.
4. Confirm the deployment by click “Start deployment”.

When a Software deployment has started it will be listed as a Job in the Jobs table (see Section 5.4). Jobs can be scheduled while creating them (see step 3). Therefore following scheduling options are possible:

Start Date	The first day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.).
End Date	The last day on which the Connectivity Suite is going to try to execute the Job, if all conditions are met (time window, day of the week etc.).
Days	Offers the possibility to constrain the execution of the Job to specific days of the week. By default, the execution is allowed for all days of the week (the blue color indicates a selected day)
Start Time	Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 0-23, the default value is 0 (midnight).
End Time	Offers the possibility to constrain the Job execution to a certain time frame within a day. Only the hour can be specified, higher precision is not supported currently. Allowed values are 1-24, the default value is 24 (midnight).

5.4 Jobs overview

All scheduled Jobs will be listed in an overview table on the page “Jobs”. This helps to manage the pending updates and provides an overview for the Jobs which were executed or not executed. In the Main dialogue box all Jobs are listed (incl. the status). By selecting a Job in the Main dialogue box, the Job details are displayed in the Detail dialogue box (see Fig. 5.11).

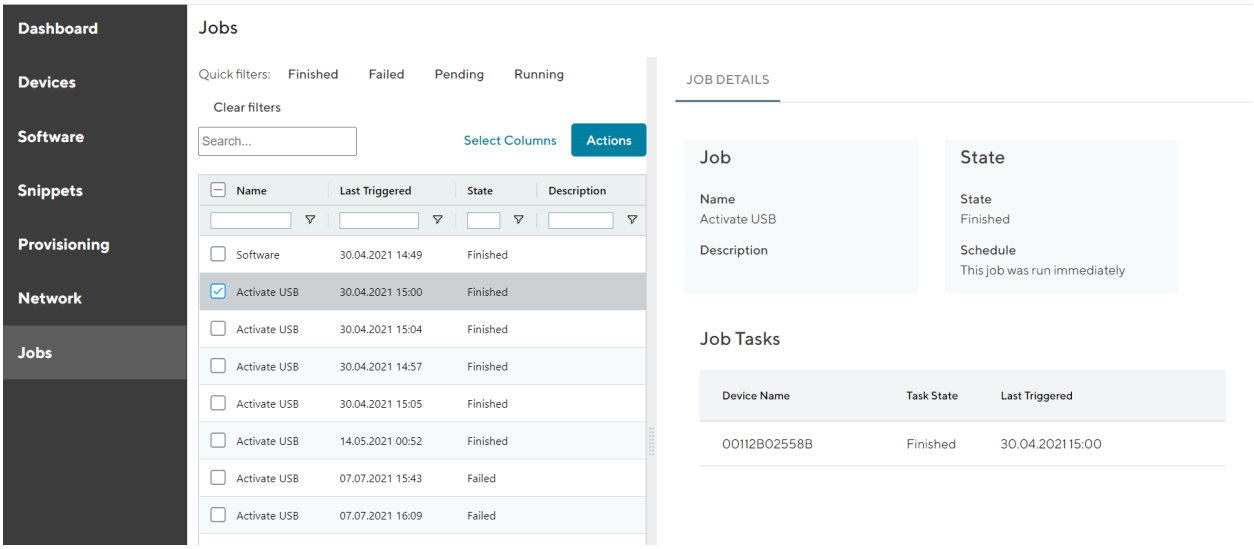

Fig. 5.11: Jobs overview

In the Detail dialogue box the Job Details are displayed:

Job	Shows the name and the description of the Job. Used for identifying a Job.
State	Shows the state of a Job. The different states are described in Section 5.4.1. Also shows whether a job was started immediately or scheduled.
Job Tasks	Shows which units are affected by the job and the job status for each unit. The different states are described in Section 5.4.1. The timestamp of when the Connectivity Suite last executed the job is also visible.

5.4.1 Job and Task states

Jobs as well as Tasks can be in one of four different states.

Pending: A Job/Task is currently waiting for the permission to execute. A Job/Task can be in this state because the start date has not been reached yet or the execution time window is currently closed (the current time is not between start and end time and/or the date of the week does not allow the execution).

Running: The deployment Job/Task is currently being executed.

Finished: The deployment Job/Task was successfully executed, this means that the Software/Configuration has been successfully deployed to the Device and the installation has been started. The correct installation of the Job cannot be verified. A Job is only considered finished if all its Tasks have the state finished.

Failed: A Job/Task is considered failed if the last possible deployment attempt, considering all specified constraints, failed. A Job with at least one failed Task is considered failed.

5.5 NM Router exchange

A NM router will be exchanged due to a defect or a hardware update etc. If the replaced Device is not the same type as the replacement Device this procedure might won't work.

Warning: Ensure that the software used on the replacement Device is the same or newer than the software version of the Device being replaced, otherwise the replacement will not work and both Devices will be lost.

1. Navigate to the page "Devices" and click on "Actions" and "Replace Device" to exchange a Device.

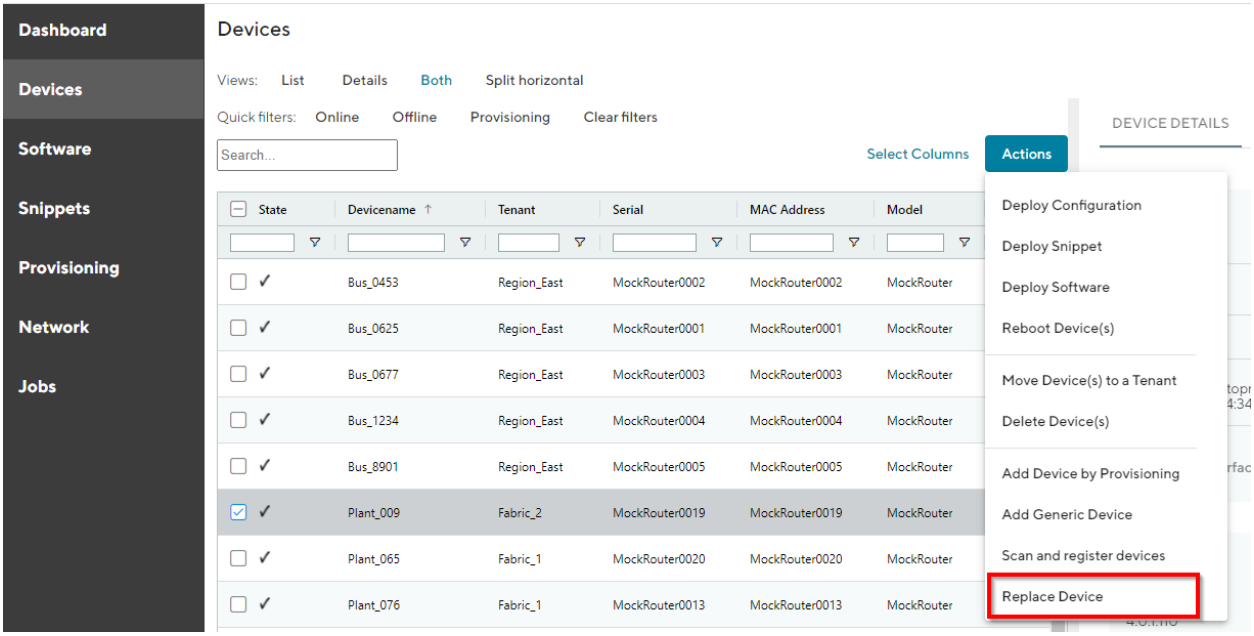

Fig. 5.12: Replace Device

2. Click "Generate Replacement Device Configuration" to generate a configuration which can be uploaded to the replacement Device.
3. Click "Download this configuration" (configuration can be uploaded via the web manager) or "Download this Configuration as USB version" Configuration can be uploaded via an usb stick) to download the configuration.
4. Upload the configuration to the replacement Device via web manager or USB, the replacement Device will automatically connect to the Connectivity Suite and the Device which will be replaced will be automatically removed from the Connectivity Suite.
5. If the device has connected correctly you can see all the Device details by clicking on the replacement device in the table of the Main dialogue box. The serial number must have changed but the rest of the information should remain the same (except for the software version).

The Connectivity Suite generates a Provisioning Config based on newest stored configuration of the Device which will be replaced and when the replacement Device connects to the Provisioning server of the Connectivity Suite the replacement process will be triggered.

Changes to existing device object:

- Software version
- Serial number

Note: When the replacement device connects to the Connectivity Suite, the certificate of the defective device will be revoked and it won't be able to connect to the Connectivity Suite anymore.

CHAPTER

SIX

REMOTE MAINTENANCE

6.1 Device access

The Connectivity Suite offers two options for accessing the units via the web interface:

	Access via web proxy	Access via OpenVPN client
Access	Access via a web proxy using the "Open Web Interface" button in the device details.	Access via a OpenVPN client using the VPN IP address of the device.
Advantages	Quick and easy access.	Allowing multiple web interfaces to be opened at the same time.
Disadvantages	Only one web interface can be opened at a time. To access a device a domain name instead of an IP address is required.	An OpenVPN client is required

6.1.1 Device access via Web Proxy

The Connectivity Suite web proxy enables access to the web interface of the devices connected to the Connectivity Suite OpenVPN servers without having to run an OpenVPN client locally. To access the web interface of the devices click on the "Open Web Interface" button in the Device Details (see picture).

Note: A subdomain called "devices" (devices.<Connectivity Suite domain>) is needed which points to the IP address of the server where the Connectivity Suite is installed. This means a corresponding DNS entry needs to be created.

6.1.2 Device access via OpenVPN client

To access the connected Devices the Connectivity Suite provides OpenVPN to access these Devices. A VPN connection to the Provisioning, the Home or Tenant Server must be established. This means the user needs to run an OpenVPN client. The configuration and certificates needed for the VPN connection can be downloaded from the Connectivity Suite via the Service Access function.

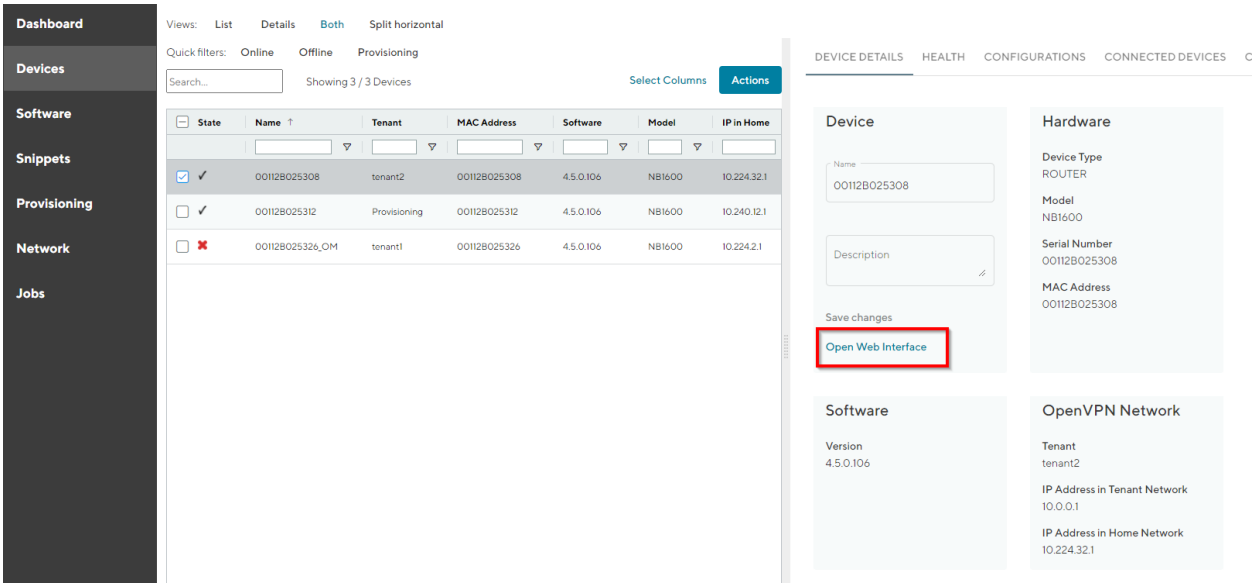

Fig. 6.1: Open web interface via web proxy

Installing OpenVPN Client

The OpenVPN client to access the devices can be downloaded from https://openvpn.net/community-downloads/.

Warning: Only the Community Download of the OpenVPN client will work if you have downloaded the OpenVPN Connect client you will not be able to connect to the Devices which are connected to the Connectivity Suite

OpenVPN access

There are three types of Service Access:

1. Tenant: The user can only access Devices (and their End Devices) which are assigned to the connected Tenant. As he is a member of this Tenant's internal network, he must use the Tenant-internal addresses to reach his destinations.
2. Home Server: The user can access every Device (and its End Devices) Tenant independent. As the user is a member of the Home Network, he must use thee home network's addresses to reach his destinations. Devices connected to the Provisioning server cant be accessed.
3. Provisioning Server: The user can only access Devices (and their End Devices) which are assigned to the provisioning server. As he is a member of this Tenant's internal network, he must use the Tenant-internal addresses to reach his destinations.

Note: For the following steps an account with Platform Administrator rights and an OpenVPN client is required.

1. Navigate to the page "Network" of the Connectivity Suite. Select the network where the required Device is assigned.
2. Click on "Download OpenVPN client configuration" at the Detail dialogue box to download the VPN certificates and configuration for an OpenVPN client.

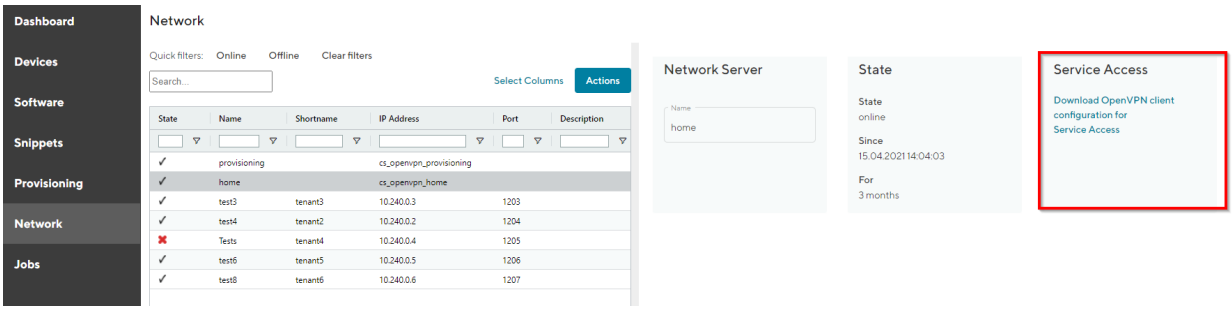

Fig. 6.2: Download VPN config

3. Start the OpenVPN client on your client pc and upload the downloaded file from step 1 into the OpenVPN client to establish a connection with the Connectivity Suite (The OpenVPN client can be downloaded from https://openvpn.net/community-downloads/).
4. After the connection has been established Navigate to the page “Devices” and select the required Device in the main dialogue table.
5. Use the IP-address shown in the Detail dialogue box to access the device.

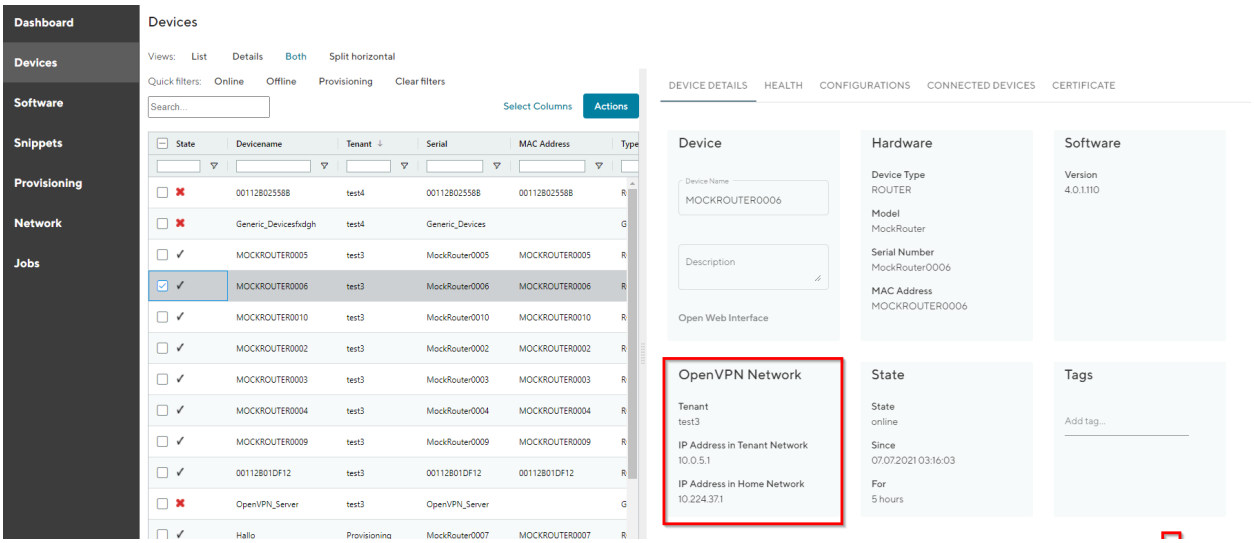

Fig. 6.3: Open web interface

CHAPTER

SEVEN

NETWORK ARCHITECTURE

When setting up the Connectivity Suite, you need to provide two non-overlapping IP ranges for the Core Network and the Home Network:

- The Core Network must be a /20 network (4'096 addresses).
- The Home Network can vary and depends on the number of connected Devices to the CS. It can be roughly estimated like this:

  Maximum number of Devices X average number of End Devices behind a single Device. For example, a /16 network (65'536 addresses) can address 4096 routers with 16 End Devices each or 2048 routers with 32 End Devices each.

7.1 Configuring the Home Network

Warning: The following network architecture settings can only be done once, during the initial setup of the Connectivity Suite!

Once a range for the Home Network has been chosen, we must determine how its addresses are distributed among the Tenants (remember that every router is assigned to a Tenant).

7.1.1 Choose a layout for the Home Network

A Tenant can manage a certain amount of IP addresses. For various reasons (network fragmentation, routing complexity), it would be impractical to set this amount for each Tenant individually. Instead, we define different types of Tenants, where each type stands for a certain amount of IP addresses manageable. Either one, two or three different types of Tenants are possible, resulting in the following three layouts:

Layout 1: Only one Tenant type

The whole address space of the Home Network is evenly distributed among the Tenants, resulting in one Tenant pool:

Layout 2: Two types of Tenants

The address space of the Home Network is split in two halves, one for each Tenant type. Each of these halves' address space is evenly distributed among the Tenants of the respective type, resulting in two Tenant pools:

Layout 3: Three types of Tenants

The address space of the Home Network is split into three parts, one for each Tenant type. One part contains half of the address space, the other two parts a quarter of the address space each. Each of these parts' address space is evenly distributed among the Tenants of the respective type, resulting in three Tenant pools:

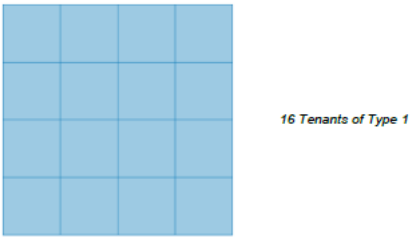

Fig. 7.1: Tenant type 1

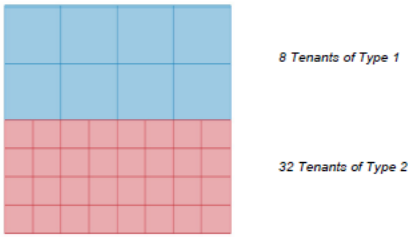

Fig. 7.2: Tenant type 2

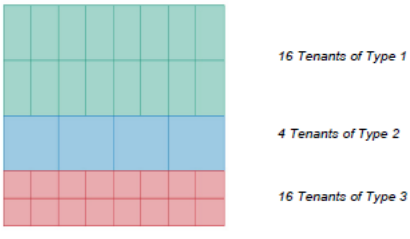

Fig. 7.3: Tenant type 3

7.1.2 Configure the Tenant types

Once a layout for the Home Network has been chosen, the Tenant types must be configured. Depending on the layout, there are one, two or three of them.

For each Tenant type, the following properties must be specified:

- A name to identify the Tenant type in the UI.
- The size (number of IP addresses) of a Tenant of this type. As the size of the relevant Tenant pool is fixed, the larger the size of a Tenant type is, the less Tenants of this type will be available. As an example, the Fig. 7.3 shows that the same pool size can be distributed among 4 Tenants of type 2 or 16 Tenants of type 3.
- The default network specifies the internal network of a Tenant of this type.
- The default number of End Devices per router is explained in chapter Section 7.1.3.
- The default maximum number of concurrent Service Access users accessing a single Tenant of this type.

The default values can be overwritten when new Tenants are created in the Connectivity Suite, i.e. these properties can be set per Tenant.

7.1.3 Setting the number of End Devices behind routers

Just as the IP address range of a Tenant pool must be evenly distributed among its Tenants, the IP address range of an individual Tenant must be evenly distributed among the routers assigned to this Tenant. The number of IP addresses each router gets depends on how many End Devices behind a router should be accessible. As a Tenant has a fixed amount of IP addresses, the less End Device addresses are needed, the more routers can be attached to that Tenant and vice versa. If one doesn't need to access any End Devices at all, then each address of the Tenant's address space can be assigned to an individual router.

It would be impractical to set the amount of End Device addresses for each router individually. Instead, this amount is configured when a new Tenant is created. All routers assigned to the same Tenant share the same amount of accessible End Devices.

As an illustration, this figure shows two Tenants of the same size (i.e. they are of the same Tenant type), but with a different End Devices per router ratio:

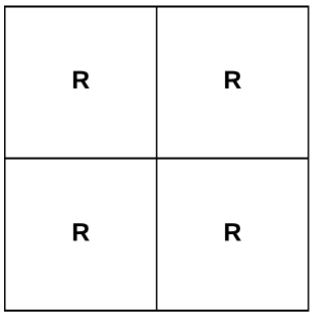

Fig. 7.4: Few routers with many End Devices each

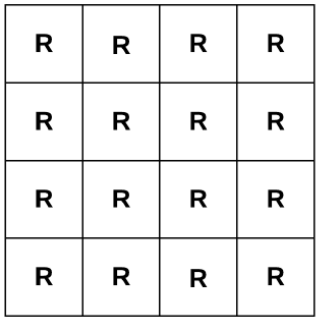

Fig. 7.5: Many routers with few End Devices each

7.2 A network configuration example

Let's look at a specific network configuration, and how to set it up during the installation of the Connectivity Suite.

We assume that we have an unused range in our private network from 10.224.0.0 upwards. We want to reserve the range up to 10.239.255.255 for the Home Network, immediately followed by the Core network:

- Core network: 10.240.0.0/20 (remember that it must be a /20 network)
- Home Network: 10.224.0.0/12

We are then asked to subdivide the Home Network. We choose to have three types of Tenant:

- The first type, allocating half of the Home Network space, is named "Medium Tenant". Each Tenant of this type should have a size of 8192 addresses, resulting in a maximum of 64 Tenants of this type. We set as a default that each device on such a Tenant can address 64 End Devices, which would yield a maximum of 128 devices per Tenant. We further choose 10.0.0.0 as the default internal Tenant network and 4 as the default maximum number of concurrent Service Access users.
- The second type, allocating a quarter of the Home Network space, is named "Small Tenant". Each Tenant of this type should have a size of 2048 addresses, resulting in a maximum of 128 Tenants of this type. We set as a default that each device on such a Tenant can address 32 End Devices, which would yield a maximum of 64 Devices per Tenant. We further choose 10.128.64.0 as the default internal Tenant network and 4 as the default maximum number of concurrent Service Access users.
- The third type, allocating the remaining quarter of the Home Network space, is named "Large Tenant". Each Tenant of this type should have a size of 32768 addresses, resulting in a maximum of 8 Tenants of this type. We set as a default that each device on such a Tenant can address 256 End Devices, which would yield a maximum of 128 devices per Tenant. We further choose 10.192.0.0 as the default internal Tenant network and 4 as the default maximum number of concurrent Service Access users.

Remember that the number of Tenant types and the size of a specific Tenant type can only be set at installation time, and that the number of End Devices, the Tenant network and the number of concurrent Service Access users can be set for each Tenant individually.

CHAPTER

EIGHT

END DEVICE ADDRESSING (NAT)

8.1 What is End Device Addressing

To access End Devices via the user interface of the Connectiviy Suite the router must perform a network NAT. The reason for this is that the router uses a Local Area Network for the End Devices with corresponding IP addresses. However, the Connectivity Suite uses a Device VPN Network within a Tenant Network to connect to the devices (see Fig. 8.1). To enable communication from the Device VPN Network to the Local Area Network of the router, a NAT must be carried out. For this, the local IP range of the router must be translated into the Device VPN Network.

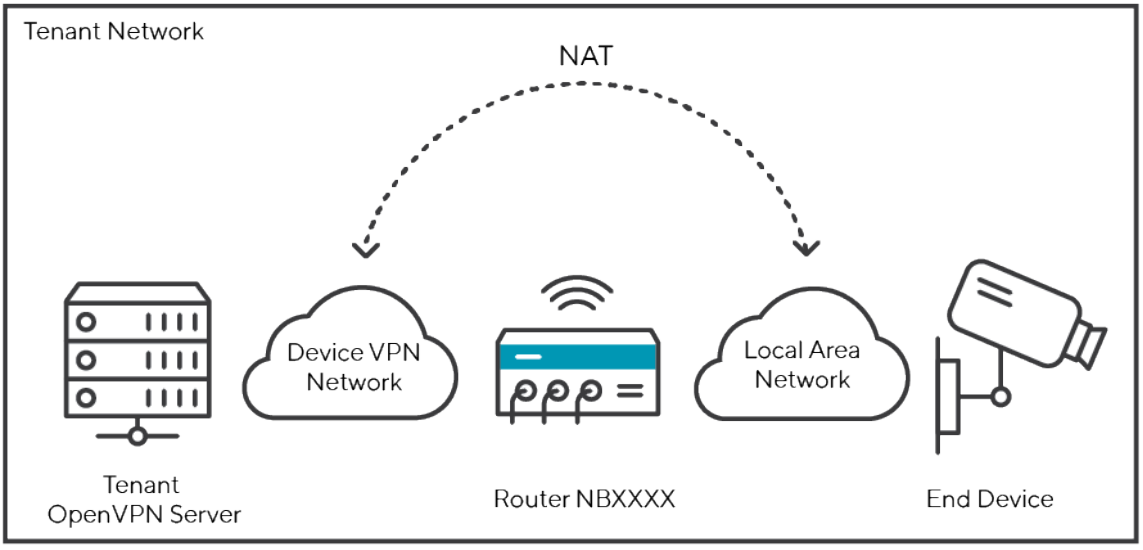

Fig. 8.1: Network setup Devices and Connectivity Suite

8.2 The Tenant Network

When adding a Tenant, you can set the size for a Tenant Network (also called Internal Network in the user interface of the Connectivity Suite) in the Connectivity Suite settings (see Fig. 8.5). The size of the Tenant Network (Internal Network) (see Fig. 8.1) defines how many devices can be connected to the Tenant. Furthermore, the Tenant Network (Internal Network) is divided into subnetworks which are called Device VPN Networks. see (see Fig. 12.1) for a graphical illustration of the Tenant Network.

8.3 The Device VPN Network

When adding a Tenant, you can define the number of End Devices to be connected to a Device (see Fig. 8.5). The defined number of End Devices defines the size of the Device VPN Network. e.g. if 256 End Devices are to be connected, the Connectivity Suite calculates the size of the Device VPN Network to /24.

However, the number of networks is limited. Since the network is a subnet of the tenant network. It is important to understand that each router has only one VPN network. Therefore, the number of Device VPN Networks that can be added also limits the number of routers that can be connected per Tenant, as only one Device VPN Network is possible per router (see Fig. 8.2).

Note: You can create more Device VPN Networks and therefore add more routers to a Tenant if you increase the Tenant Network size or reduce the number of terminals when creating a tenant.

8.4 The Network NAT

To access the End Devices, the Device VPN Network address must be translated to a Local Area Network address. As example in Fig. 8.3, the Device VPN Network 10.0.0.0/24 is translated into the Local Area Network 172.16.0.0/24.

Warning: It is important that the subnetmask of the Device VPN Network and the Local Area Network are the same, otherwise the NAT will not work.

8.5 Use Case Example

An example of what a real-world scenario could look like is explained below.

Assumption:

1. Each End Device is assigned the IP address 172.16.0.111
2. Max. 256 End Devices will be connected to a Device
3. Max. 32 Devices will be connected to a Tenant

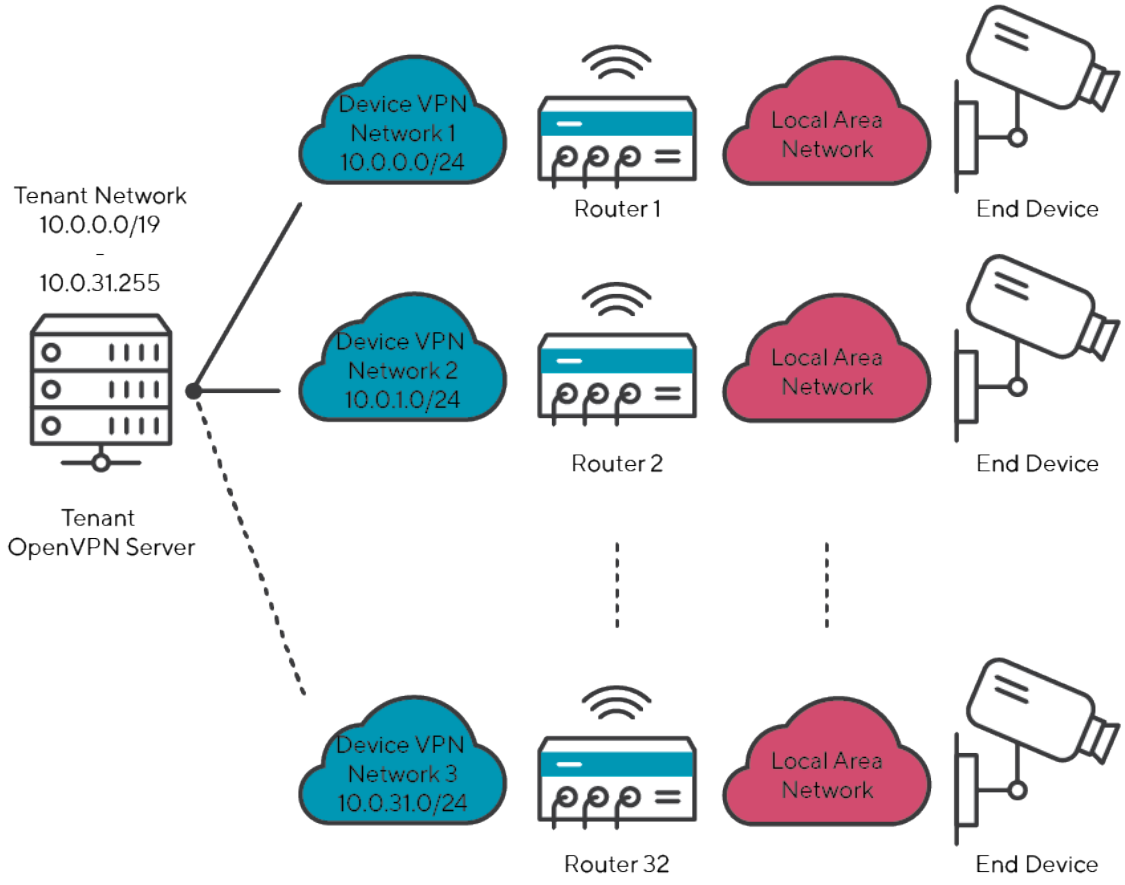

Fig. 8.2: Network Setup in Tenant Network

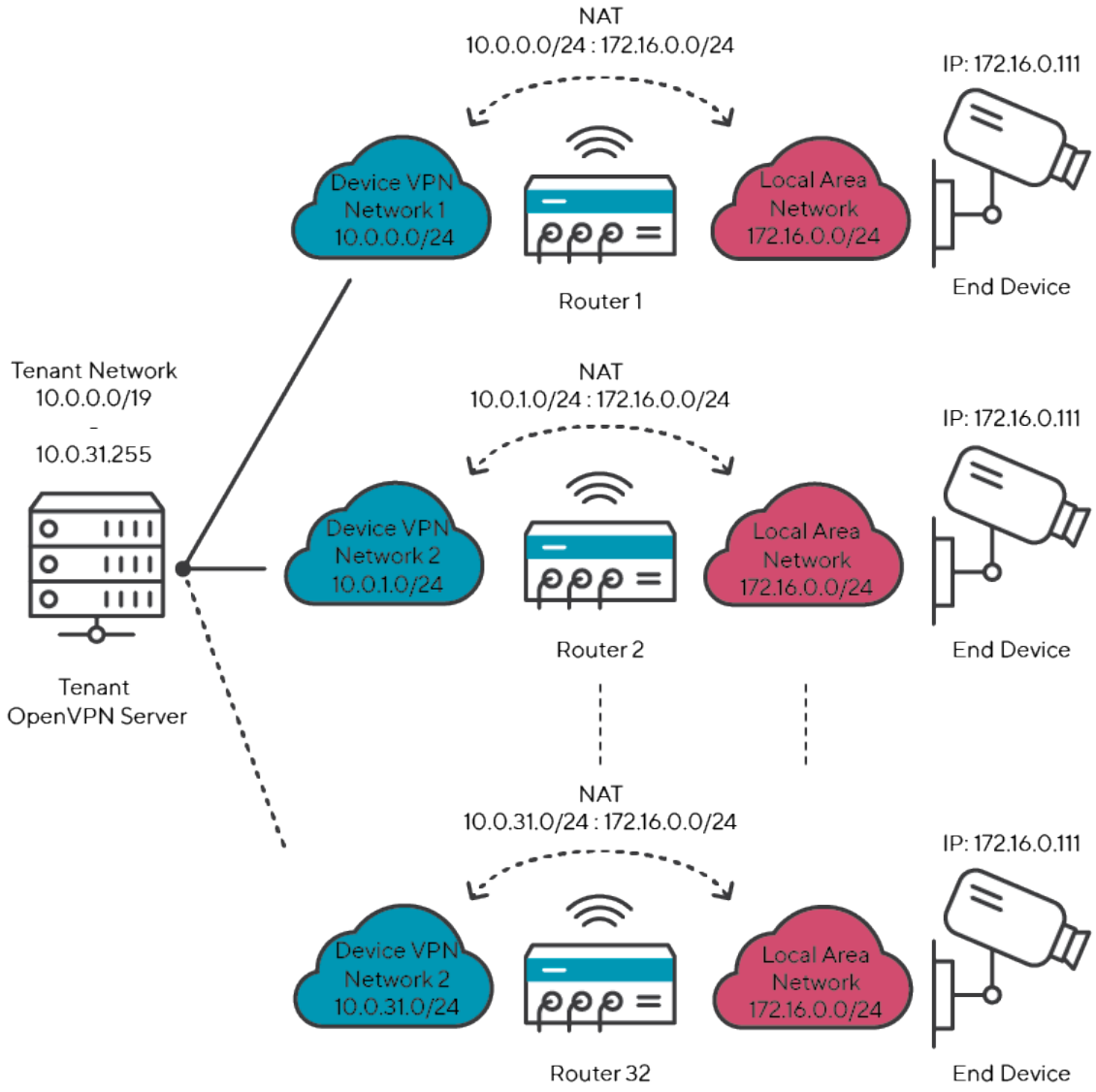

Fig. 8.3: Network Setup in Tenant Network

8.5.1 Considerations before configuration

1. To connect 256 End Devices, the Local Area Network must have a size of /24. Since all my End Devices have the same IP address of 172.0.0.111, the Local Are Network must be 172.0.0.0/24.
2. If the Local Ara Network has a size of /24, the VPN network must also have a size of /24 (the Ip address range of the Device VPN Network is freely selectable, whereby 10.0.0.0/24 is selected for this example).
3. To connect 32 routers you need 32 Device VPN Networks which have all a network size of /24 with each 256 End Devices.
4. If you have 32 Device VPN Networks and per Device VPN Network you have 256 End Devices this means you must be able to connect 8,192 devices to one Tenant Network therefore the Tenant Network size must be /19.

Result: If you want to connect 32 Devices and 256 End Devices per Device, you have to select a Tenant Network size of /19. Furthermore, you must perform a network NAT from your Local Area Network (17.0.0.0/24) to the Device VPN Network (10.0.0.0/24).

The network setup would look like Fig. 8.4.

8.5.2 Settings Connectivity Suite

In the Connectivity Suite, only the Tenant Network size and the number of End Devices needs to be defined so that the corresponding network can be set up.

8.5.3 Settings Router

In order to carry out a NAT, various steps are necessary which are explained below:

1. Open the web interface of the router, open the Firewall/Inbound Rules page and create a new rule
2. Select “network” for the mapping as it is required not only to translate an IP address but an entire subnet.
3. Select the interface. The interface must be an OpenVPN tunnel as the connection from the Device VPN Network to the Local Area Network is made via the OpenVPN tunnel of the Connectivity Suite.
4. Add the Device VPN Network as Target address/netmask.
5. Add the Local Area Network as Redirect address/netmask.
6. Save the settings. Devices that are in the Local Area Network are now displayed in the Connectivity Suite in the Device Details under Connected Devices.

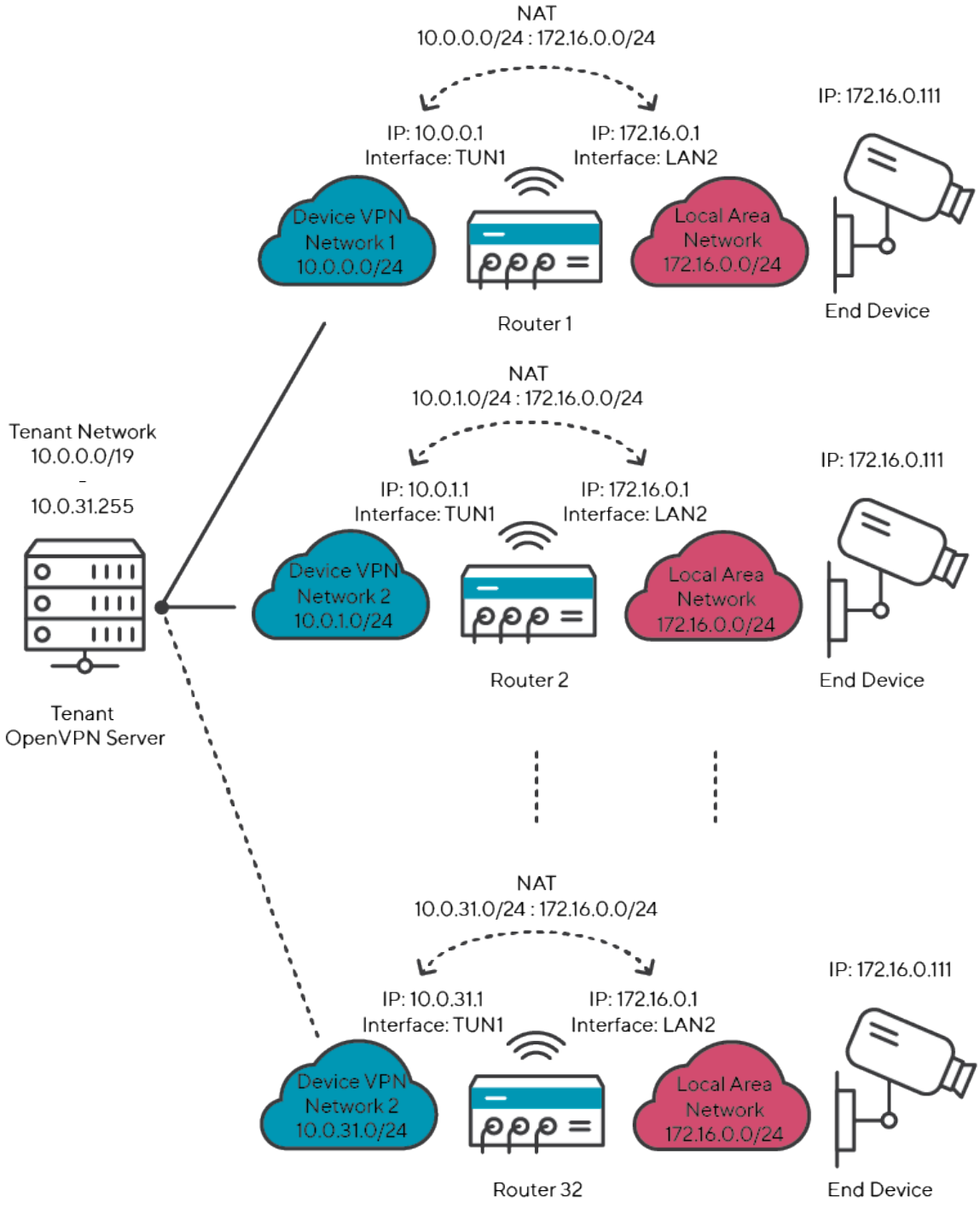

Fig. 8.4: NAT Device VPN Network to Local Area Network 2:2

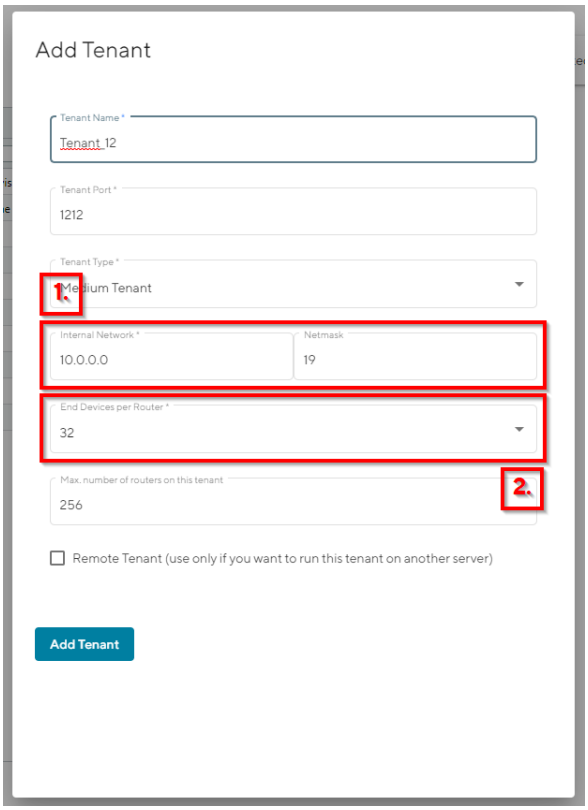

Fig. 8.5: Settings Connectivity Suite

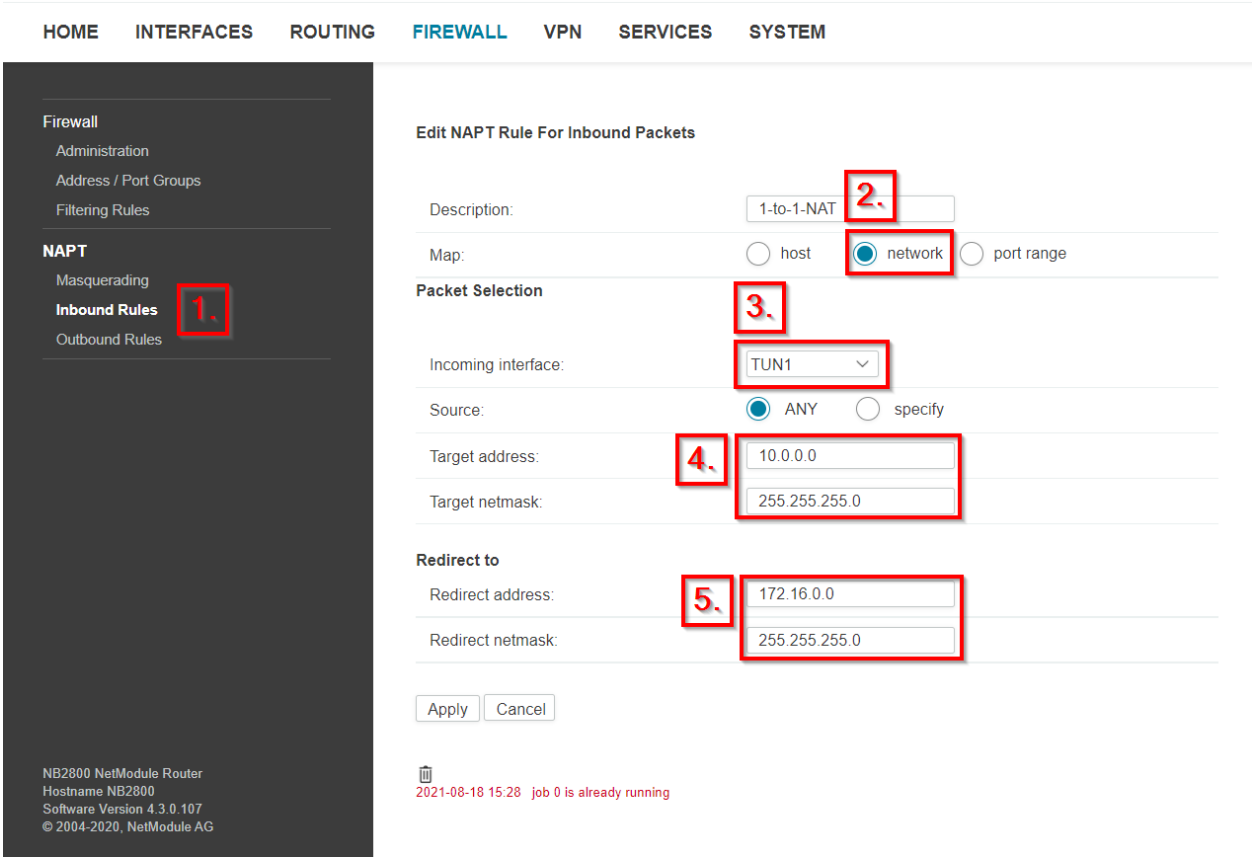

Fig. 8.6: NAT Settings NetModule Router

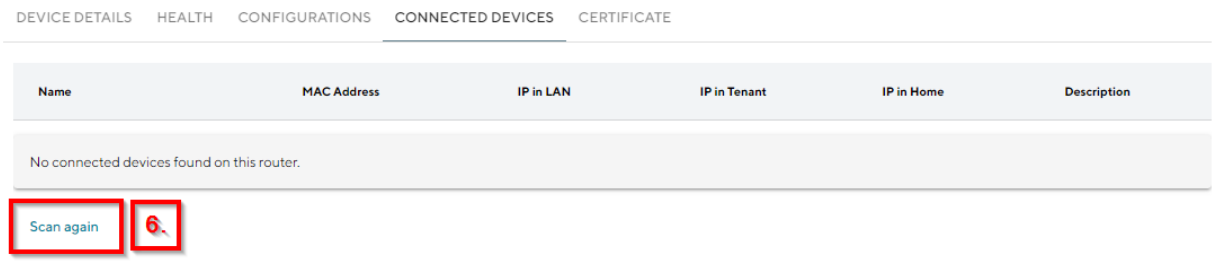

Fig. 8.7: End Devices View Connectivity Suite

CHAPTER

NINE

TROUBLESHOOTING

9.1 Troubleshoot a Device

For the following steps an account with Platform Administrator rights is required.

If there are problems with a Device, there are several things that you can check:

- Is the Device online?
  - No: Check when it was last online by navigating to the Health page and selecting the specific Device
    - Is the Device powered on?
      - Yes: Try to access the Device directly by downloading the Service Access VPN configuration and establishing a VPN connection to the Core Network
      - No: Power on the Device
- Yes, do a direct Device access by first downloading the Service Access VPN configuration and troubleshooting the Device outside of the Connectivity Suite

9.2 Troubleshoot the Connectivity Suite

For the following steps an account with Platform Administrator rights is required.

1. Click on the wrench icon in the upper right corner
2. Select “Logs”
3. Click on “DOWNLOAD LATEST” to download the latest log file or choose one or multiple older log file from the list and click on “DOWNLOAD SELECTED”. The name of the file in the table indicates the timestamp of the last log entries in the file
4. Download the file and send it to the Connectivity Suite support

9.3 General issues

9.3.1 Issues during an Update

Server certificate verification failed

Error

```
fatal: unable to access 'https://cs-dev.netmodule.com/connectivitysuite/cs-update.git/
↪': server certificate verification failed. CAfile: /etc/ssl/certs/ca-certificates.
↪crt CRLfile: none
```

Solution

Update the Linux packages using the following command via terminal on the Linux server:

Update the CA certificates:

```
sudo apt update
sudo apt-get install --only-upgrade ca-certificates
```

If that does not yet resolve the issue, update all packages:

```
sudo apt update
sudo apt upgrade --fix-missing
```

CHAPTER

TEN

USER RIGHTS MANAGEMENT

The Connectivity Suite user hierarchy consists of three different user roles.

10.1 Platform Admin

The Platform Admin is the highest in the role hierarchy. A Platform Admin can administer the complete Connectivity Suite instance. This means he can administer Tenants, Devices and users.

10.2 Tenant Admin

A Tenant Admin can only administer Devices connected to specific Tenants. A Tenant Admin can assign the Tenant Admin and Tenant User roles for Tenants he administrates to other users.

10.3 Tenant User

The Tenant User only has a monitoring function for Devices within specific Tenants. A Tenant User is not allowed to manipulate Devices.

10.4 User rights table

10.5 Assigning user rights

1. Navigate to the page “User Management” of the Connectivity Suite UI by clicking on the tool icon in the Support bar.
2. Click on “Actions” at the upper right corner of the Main dialogue box and click “Add user” to add a user.
3. Fill out the required fields and click on “Add user” to add the user.
4. The added user must now be shown in the Main dialogue box in the table.

When creating the user following parameters can be set

	User rights	can view Devices	can view health data	can manipulate Devices	can modify configurations	can execute Device updates	can create/delete Tenants	can administer users	can assign Platform Admin role	can assign Tenant Admin role for Tenant X	can assign Tenant User role for Tenant X
Roles	platform.admin	x	x	x	x	x	x	x	x	x	x
	TenantX.admin	x	x	x	x	x				x	x
	TenantX.user	x	x								

Fig. 10.1: User rights table

Fig. 10.2: Manage users

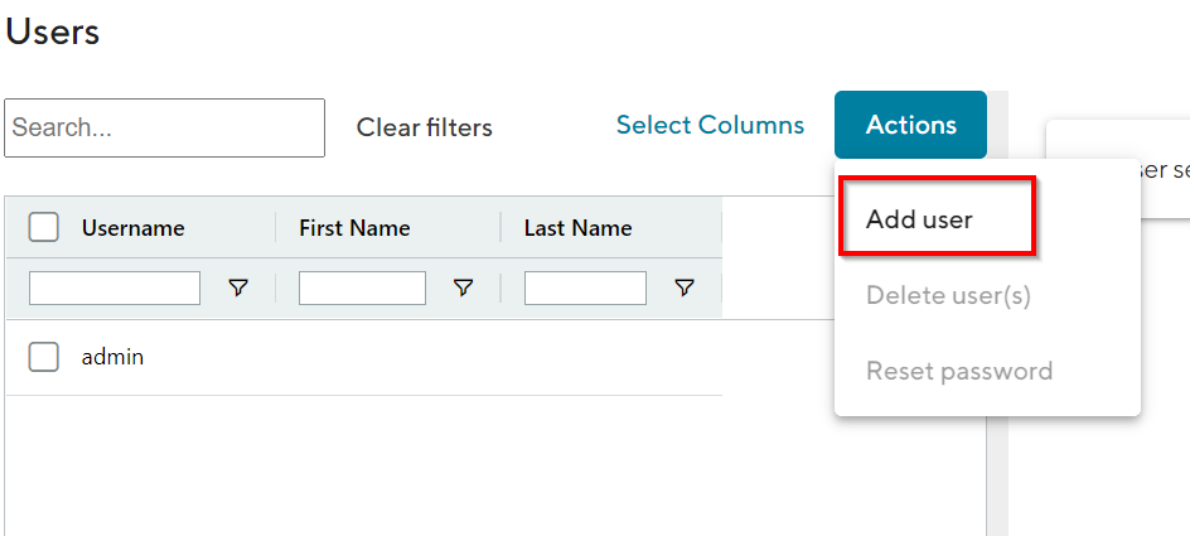

Fig. 10.3: Added user

Username	Name of the user (Login credential)
Email	Email of the user
Password	Password to login (Login credential)
First Name	First name of the user
Last Name	Last name of the user
Address	Address of the user
Company	Company the user works for
Phone	Company phone number

When the tab “User Roles” is opened in the Main dialogue box, the user rights can be assigned there.

The following settings can be made:

Platform admin	If the checkbox is set the new user will have platform admin rights
Tenant Admin	Select the Tenant of which the user will have admin rights (if no selection is taken the user won’t be a Tenant admin). See Section 10.4 for the different user rights.
Tenant User	Select the Tenant the user can access. See Section 10.4 for the different user rights.

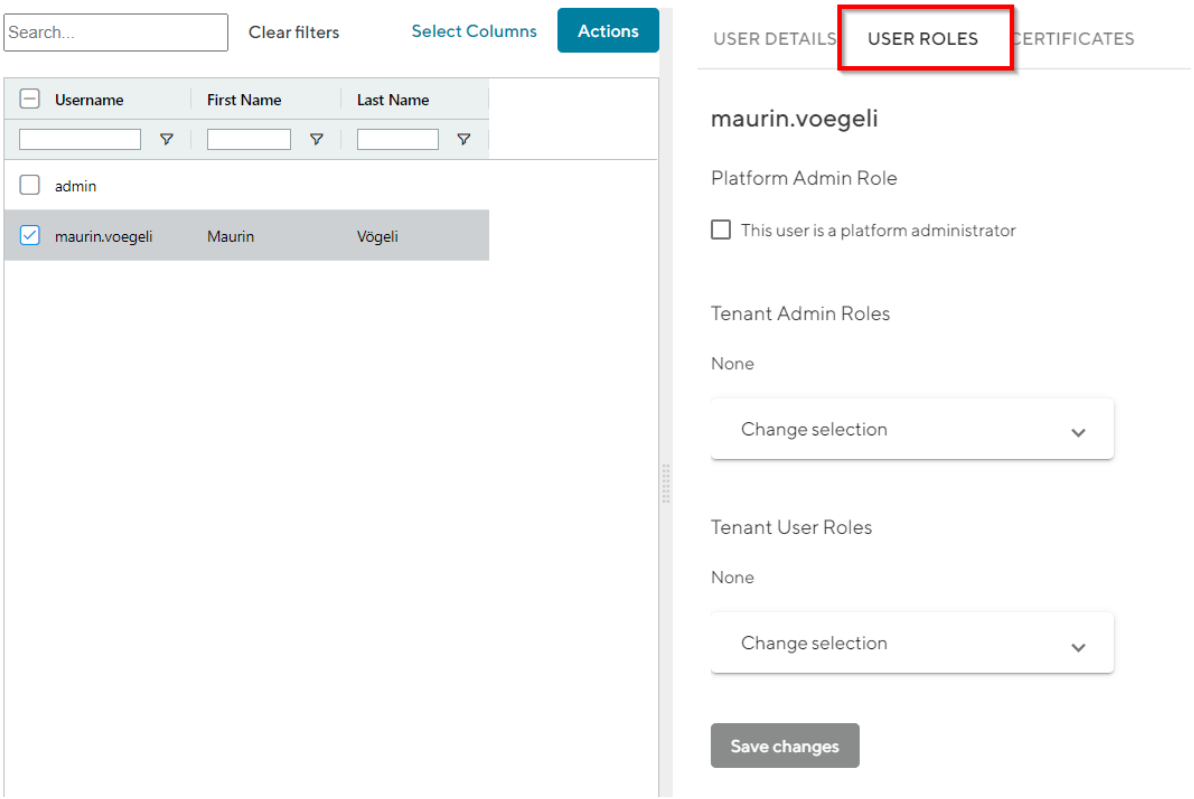

Fig. 10.4: User roles

CHAPTER

ELEVEN

UPDATE & BACKUP

11.1 Backup

Execute the python script backup.py which is stored in the scripts folder with the backup directory as parameter. This process may take a while.

Example: python backup.py cs-backups/cs-backup-01.02.2019

11.2 Restore

Execute the python script restore-and-restart.py which is stored in the scripts folder with the directory of the backup which shall be restored as parameter.

Warning: All data in the running Connectivity Suite instance is going to be overwritten during the restore process!

The Connectivity Suite will be restarted several times while the backup is restored. This process may take a while.

Example:

python restore-and-restart.py cs-backups/cs-backup-01.02.2019

11.3 Update

Warning: Only a sudo user can execute updates. Do not update while being logged in as a root user, it wont work.

1. Make a backup of the instance before starting the migration process

Note: Ensure that the Connectivity Suite is installed on a supported version of Ubuntu (see release notes) and update all packages beforehand to ensure a trouble-free update.

2. a) For the very first update in the life cycle of the instance, execute the command below in the home directory (e.g. /home/ubuntu):

```
git clone https://cs-dev.netmodule.com/connectivitysuite/cs-update.git
```

2. b) If an update has already been carried out in the life cycle of the instance, execute the command below in the home directory (e.g. /home/ubuntu):

```
git pull https://cs-dev.netmodule.com/connectivitysuite/cs-update.git
```

3. When prompted to log in to the Git repository, you can use the same credentials as when you installed the software.

Note: You should have received the credentials when ordering the software. If they are no longer available, please contact your NetModule representative.

---

4. Navigate into the cs-update folder
5. Navigate into the folder with the version to update to (e.g. 2.2.12)
6. Execute the file update-xxxx.sh (./update-xxxx.sh)

11.4 Update v2.6

Note: If you update to version 2.6, you must make a CNAME entry in the DNS server so that you can use the new web proxy feature. You can find out which settings are necessary in chapter Section 3.1.4.

CHAPTER

TWELVE

APPENDIX

12.1 System architecture IP overview

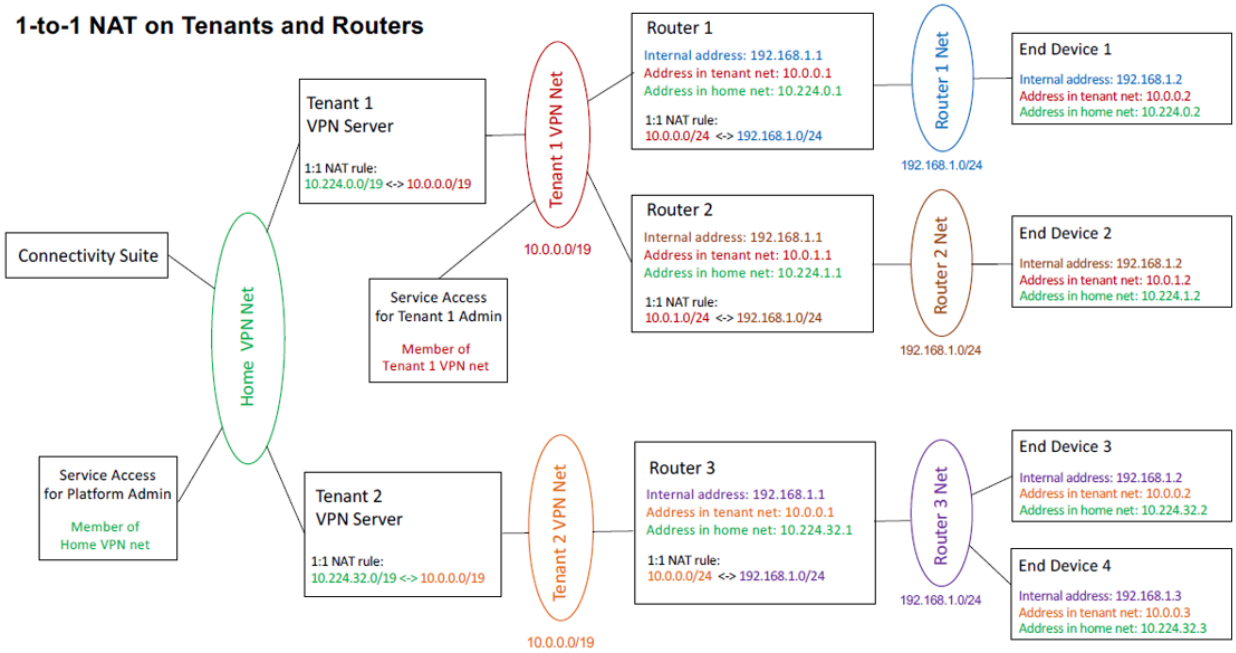

Fig. 12.1: Network architecture

NetModule AG is located at

Maulbeerstrasse 10
3011 Bern
Switzerland
info@netmodule.com
Tel +41 31 985 25 10
Fax +41 31 985 25 11

For more information about NetModule AG, visit the NetModule web site at: www.netmodule.com