# WebAccess/VPN

## APPLICATION NOTE

ADVANTECH

# Used Symbols

*Danger* – Information regarding user safety.

*Attention* – Problems that can arise in specific situations.

*Information* – Useful tips or information of special interest.

*Example* – Example of function, command or script.

Source codes under GPL or other open source licenses are available free of charge by sending an email to:

iiotcustomerservice@advantech.eu

Please see https://icr.advantech.com/devzone for more information.

# Software Version

This Application Note describes the *WebAccess/VPN* in version **1.1.4**.

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic.
Document No. APP-0021-EN, revision from March 26, 2024. Released in the Czech Republic.

# Contents


**1 Introduction** **1**

1.1 What is WebAccess/VPN . . . 1
1.2 Technical Concept . . . 1
1.2.1 Parts of the WebAccess/VPN system . . . 2
1.2.2 How is the Router Connecting to the System . . . 2
1.2.3 Security of Communication Channels . . . 3
1.2.4 Networks – Groups of Devices . . . 3
1.3 Licensing Concept . . . 4

**2 Installation of WebAccess/VPN** **5**

2.1 Free Demo Installation on Amazon AWS . . . 5
2.2 Installation on Amazon AWS . . . 6
2.3 On-Premises Installation – VirtualBox . . . 10
2.4 VPN-BOX-UNO Installation . . . 16
2.5 Installation Wizard . . . 17
2.6 Performance Scaling Recommendations . . . 24
2.6.1 Amazon Instance Type . . . 24
2.6.2 Standalone Hardware . . . 24
2.7 Security Update Patch for Frontend . . . 25

**3 Configuration of Advantech Router** **26**

3.1 Upload Router App (User Module) VPN Portal . . . 26
3.2 Connect the Router to WebAccess/VPN . . . 27
3.3 Validate the Router on WebAccess/VPN . . . 28
3.4 Set the Router Access Policy . . . 28
3.5 Router App (User Module) Status and Log Messages . . . 29
3.5.1 Router App (User Module) Log Messages . . . 30

**4 WebAccess/VPN User Interface** **31**

4.1 Login to WebAccess/VPN . . . 31
4.2 Dashboard . . . 31
4.3 Routers . . . 32
4.3.1 Routers: Edit . . . 35
4.3.2 1:1 NAT . . . 42
4.3.3 Firewall Rules for Router . . . 46
4.3.4 Routers: Link . . . 46
4.3.5 Routers: Delete . . . 47
4.4 Networks . . . 48
4.4.1 Edit – Firewall Rules for Network . . . 49

4.5 Devices in Networks . . . . . 51
4.6 Firewall Rules . . . . . 52
4.7 Standalone VPN Clients . . . . . 53
4.7.1 Standalone VPN Clients: Edit . . . . . 55
4.7.2 Control Standalone VPN Client Service . . . . . 56
4.8 Administration . . . . . 57
4.8.1 Application . . . . . 57
4.8.2 Pre-validation . . . . . 60
4.8.3 Settings . . . . . 61
4.8.4 Users . . . . . 64
4.8.5 Logs . . . . . 66

**5 Advanced Management 67**

5.1 Password Reset . . . . . 67

**6 Troubleshooting 68**

6.1 How to check WebAccess/VPN Running Services . . . . . 68
6.2 How to Access Logs . . . . . 68

**7 Related Documents 69**

**A Standalone Hardware Test 70**

# List of Figures


1 The basic parts of the WebAccess/VPN system, showing a new router connection 2
2 Networks – groups of routers . . . 3
3 Router App *VPN Portal* after upload to the router . . . 26
4 Router app menu . . . 26
5 *VPN Connection* configuration page – Dispatch Server IP . . . 27
6 Validating the router in WebAccess/VPN Web UI . . . 28
7 *VPN Portal* status page of the validated router . . . 29
8 *OpenVPN Tunnel* status page of the validated router . . . 29
9 Example of a new tunnel network interface and Route Table . . . 29
10 Login to WebAccess/VPN . . . 31
11 WebAccess/VPN Dashboard . . . 31
12 Routers in WebAccess/VPN . . . 32
13 Routers – Overview of a Router . . . 34
14 Routers – main page of a Router – Edit LANs . . . 35
15 Routers – General tab of a Router . . . 37
16 Routers – Networks membership of a Router . . . 38
17 Routers – Proxy settings of a Router . . . 39
18 Routers – Firewall Rules . . . 40
19 Routers – Actual Settings of a Router . . . 41
20 Routers – Connection Log of a Router . . . 41
21 Routers – 1:1 NAT Interface Mode . . . 42
22 1:1 NAT Example 1 . . . 43
23 1:1 NAT Example 2 . . . 44
24 1:1 NAT Example 3 . . . 45
25 Device Firewall rule example . . . 46
26 Routers – Link: login to Router via WebAccess/VPN as proxy . . . 47
27 Networks in WebAccess/VPN . . . 48
28 Networks – Network overview . . . 48
29 Networks – Firewall Rules . . . 49
30 Device Firewall rule example . . . 50
31 Devices in Networks . . . 51
32 Devices in Networks – add the device to network . . . 51
33 Firewall Rules . . . 52
34 Manage Standalone VPN Clients . . . 53
35 Add a Standalone VPN Client dialogue . . . 54
36 Edit Standalone VPN Client – General . . . 55
37 Edit Standalone VPN Client – Proxy . . . 56
38 Administration submenu . . . 57
39 Application Management . . . 57
40 Upgrade WebAccess/VPN Server . . . 58

41 Update license of WebAccess/VPN Server . . . . . 58
42 WebAccess/VPN services management . . . . . 59
43 Download router apps for routers . . . . . 59
44 Logs . . . . . 60
45 Settings of WebAccess/VPN . . . . . 61
46 Users management . . . . . 64
47 User Edit . . . . . 64
48 Logs . . . . . 66

# List of Tables

1 Routers properties . . . . . 33
2 Devices – LANs Interface Modes . . . . . 35
3 Device Firewall rule – options and syntax . . . . . 47
4 Network firewall rule – options and syntax . . . . . 50
5 WebAccess/VPN Settings items . . . . . 63
6 Performance test results . . . . . 70

# 1. Introduction

## 1.1 What is WebAccess/VPN

The *WebAccess/VPN* (VPN = Virtual Private Network) is a complementary management and monitoring tool for the secured interconnection of Advantech routers and the LANs behind them. *WebAccess/VPN* provides services like *clustering the routers into separate groups* (called Networks, allowing some routers to communicate with each other), *accessing the router's web interface* from the Internet, and *accessing the devices behind the routers*.

The architecture of *WebAccess/VPN* was designed to be:

- Scalable – can handle thousands of routers.
- Flexible – easily manageable, can be hosted by the customer.
- Secure – the architecture withstands the usual attack vectors. The network traffic runs through **OpenVPN** tunnels.

Other notes:

- For permitting public hosts access to internal servers, **1:1 NAT** can be used.
- **Firewall** filtering rules can be created separately for devices and for entire groups of devices (called Networks).
- The **Standalone VPN Clients** service enables external secured connections to *WebAccess/VPN*.
- **User management** with different user roles is supported.
- Both **v2 and v3** Advantech **routers are supported**. Configuration of the router is not complicated – upload the router app. OpenVPN settings are then pushed to the router automatically after validation.

## 1.2 Technical Concept

The basic principle is that all the routers are connected directly to *WebAccess/VPN* via OpenVPN tunnels. Rules for mutual access (Networks – groups of devices, see Fig. 2) can also be created. Additional VPN tunnels can be made (Standalone VPN Clients) so any other device (Windows, Linux, Smartphone, etc.) can access the secured network.

### 1.2.1 Parts of the WebAccess/VPN system

The elements of one *WebAccess/VPN* instance are as follows:

- **Devices** – Routers or Standalone VPN Clients are the leaf elements. The Router app *VPN Portal* has to be uploaded to the router. The routers are then connected to these two entities:
- **Dispatch Server (DS)** – a registration service that holds the current IP address of the Customer Server (CS). Whenever routers have problems locating their CS, they can contact the DS for its current address and credentials. The Dispatch Server is used only when Routers don't know the Customer Server address.
- **Customer Server (CS)** – is a central traffic point for interconnected devices. Routers are organized into groups called Networks, prescribing which Routers may interconnect to which others.

> In version 1.1.0, the Dispatch Server (DS) and Customer Server (CS) both run on the same machine. In the later versions, it will be possible to run them separately.

### 1.2.2 How is the Router Connecting to the System

As shown in Figure 1 below, the router first contacts the Dispatch Server (DS). The Dispatch Server's role is to give the router a Customer Server (CS) address. A successful case is described here. The Router then connects directly to the Customer Server (CS), an OpenVPN server with Web UI that controls traffic. Finally, the CS lists the Router as a new router waiting for validation.

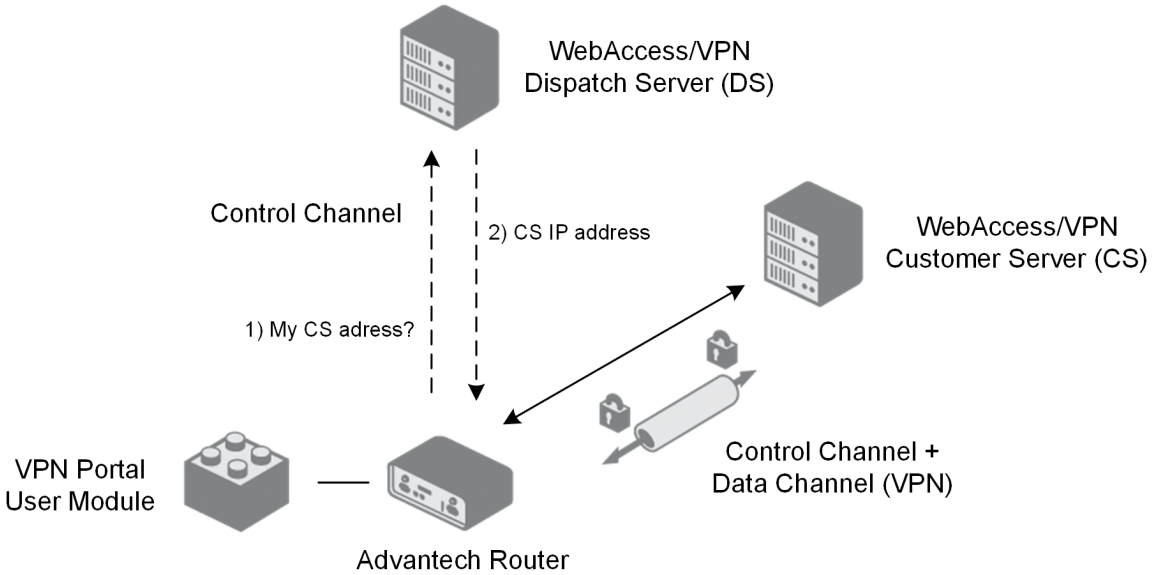



Figure 1: The basic parts of the WebAccess/VPN system, showing a new router connection

After the router is **manually validated** (granted access) by the administrator on the Customer Server (CS), the Customer Server (CS) provides OpenVPN credentials to the router and can force the configuration of LAN addresses (if set so manually by the administrator). The **router** (and its LANs) **can now be added manually** by an administrator **to a Network** where they can access its networked colleagues and their LANs.

### 1.2.3 Security of Communication Channels

All Web user interaction is secured by HTTPS protocol (accessing WebAccess/VPN, managing single router Web interface, where CS serves as proxy). When a router is connecting for the first time to WebAccess/VPN (for validation), there is a temporary SSL/TLS channel for registration and exchange of OVPN credentials. After the OpenVPN tunnel is established, both the control channel and any network traffic are transmitted within the tunnel.

### 1.2.4 Networks – Groups of Devices

The local network behind a Router is called a LAN. A group of devices (Routers and Standalone VPN Clients), which can communicate with each other, is called a Network. All validated Routers (and Customer Server) are part of the "VPN Network". See an example of such a network in Figure 2, including example IP addresses.

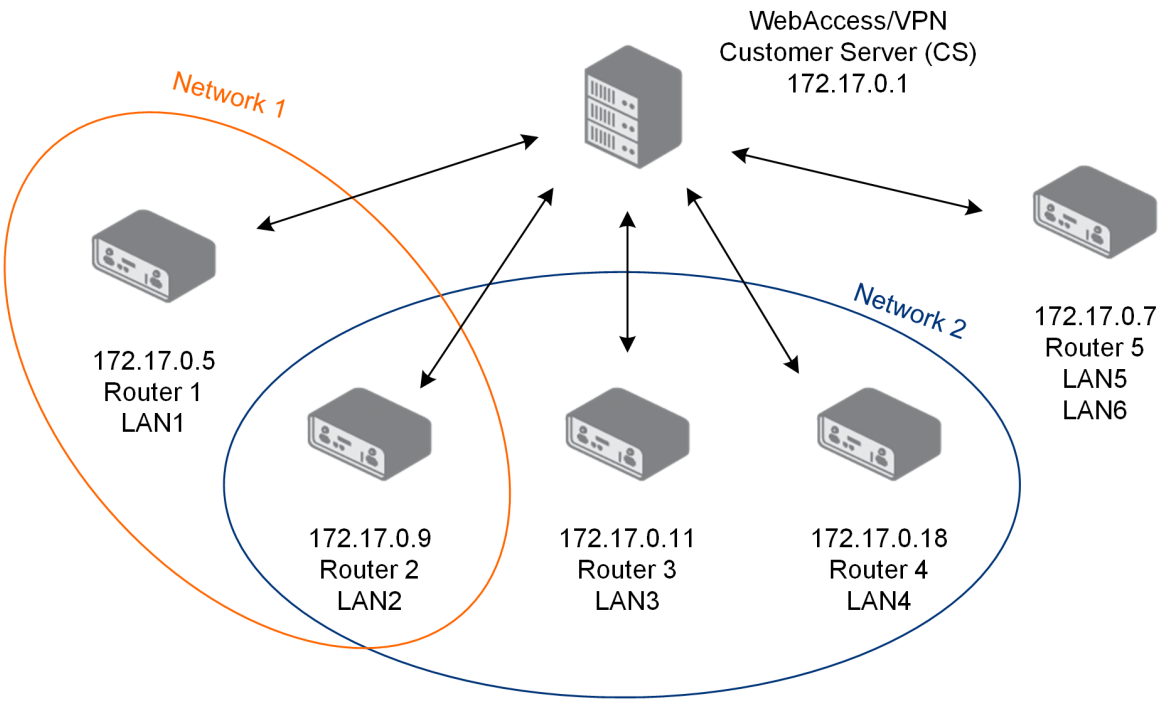



Figure 2: Networks – groups of routers

Routers' LANs can be configured at the Customer Server. Also, Networks (Network 1, Network 2) are configured on the Customer Server. Any Router can be a member of multiple Networks. The configuration is stored in the database on the Customer Server. Configuration changes (LANs range, Networks routing) are propagated to Routers when possible.

## 1.3 Licensing Concept

The default license will be installed with WebAccess/VPN. This allows a customer to connect 5 devices and create 2 VPN standalone clients, so all the features can be tested.

To order your license, please contact your local Sales Representative. The license can be updated anytime on WebAccess/VPN *Administration – Application* page, see Chapter 4.8.1.

# 2. Installation of WebAccess/VPN

WebAccess/VPN for now does not work with routers with firmware version 6.3.10. Last functional firmware version is 6.3.9

## 2.1 Free Demo Installation on Amazon AWS

The free demo version from Amazon AWS is limited to 5 routers, including 2 standalone VPN clients. For example, in practice, you can have 3 routers and 2 standalone VPN clients for a total of 5 items. This version is not intended for production usage and can not be upgraded or licensed to the production version.

The free version of the product is no longer available on Amazon Marketplace. From now on, follow the installation guide as instructed in Chapter 2.2 and then Chapter 2.5.

For usage with the purchased license, you can select from these installation options:

- A **customer-managed** installation from an image on the **Amazon AWS** cloud.
  Follow Chapter 2.2 and then Chapter 2.5.
- **On-premises** installation as **VirtualBox appliance**.
  Follow Chapter 2.3 and then Chapter 2.5.

## 2.2 Installation on Amazon AWS

Installation is done from a shared AWS (Amazon Web Services) image with an install wizard for an easy start, so the customer can install and control his WebAccess/VPN installation. The customer manages the certificates and keys, and Advantech has no access. The installation process is described below.

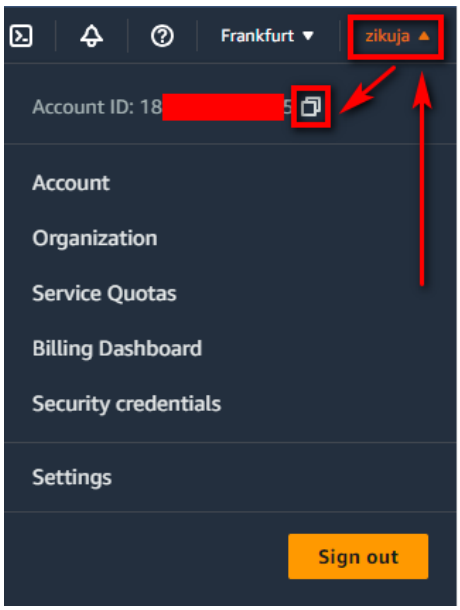
**Prerequisites for the install:**

- An **Amazon AWS account** is required to launch your Amazon instance from the image provided. A free account is sufficient for a trial, but be aware that fees may apply.
- A **domain name** for your WebAccess/VPN installation is needed. This will allow the *Link* (Proxy) feature described in Chap. 4.3.4 working. Advantech can provide a domain name (subdomain of vpnportal.cloud domain). Consider if you want to set up your own domain name or if you want to use one provided by Advantech.

Note that interaction with the customer is required before the installation itself so that Advantech can share the installation image with the customer – see the first step below.

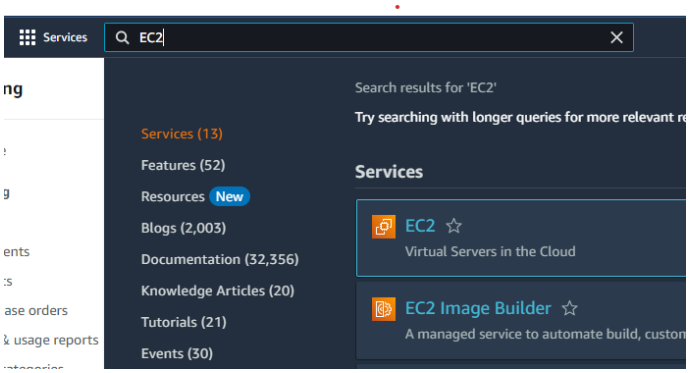
1. Login to your Amazon AWS account (https://aws.amazon.com) and select *My Account* from the profile menu.

   Copy your **Account ID**, and please send it with your **Region** to Advantech using the following email address: AEU.CZ-VPN-aws@advantech.com

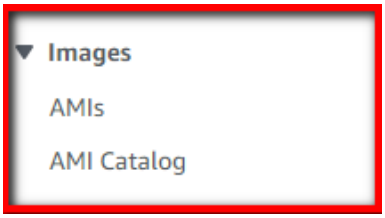



   Wait for a confirmation email that the installation image was shared with your Amazon AWS account.

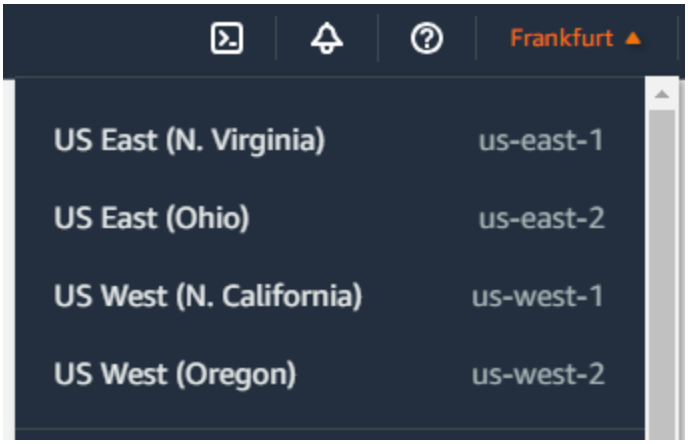
2. Now login to your Amazon AWS account and select Services, **EC2**.



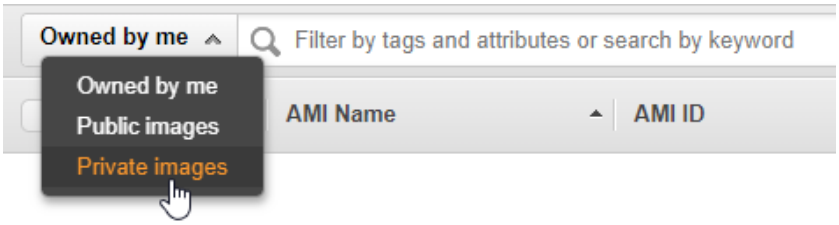

3. Select the **AMIs** form Images menu on the left.




4. Switch your location to **Frankfurt** at the top right corner. Should you want to use a different location, please contact Advantech using the following email address: AEU.CZ-VPN-aws@advantech.com.
   The image will then be copied to your location.

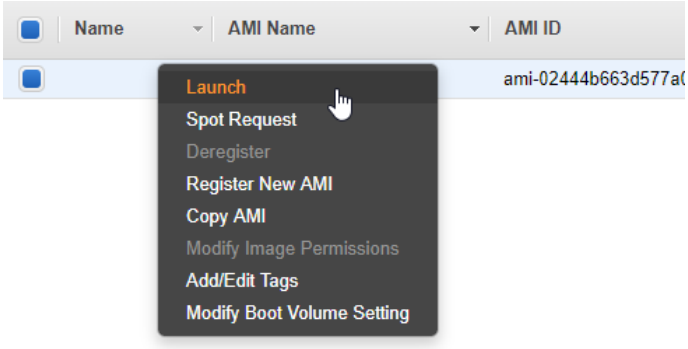


5. Change the filter of images to **Private images**.

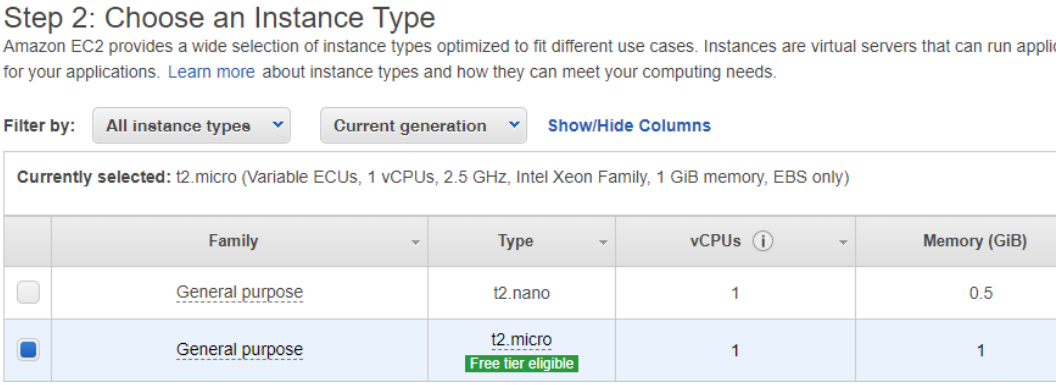



6. Now, the shared image from Advantech should be visible under the name **WebAccess/VPN**. You can also check the owner of the image is 686278836833.
7. Right-click on the image and select *Launch* to create the instance.

> Do not stop the instance once running. Stopping the instance may lead to a loss of public IP address and the WebAccess/VPN data in this instance.




8. In the next step (*Step 2: Choose an Instance Type*) select **t2.micro** type (for free account) or follow the performance scaling recommendations Chapter 2.6.



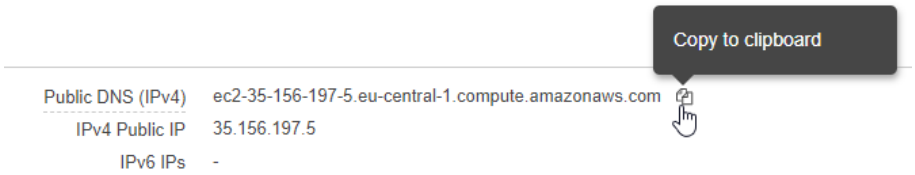

You can use default settings (or desired) for the next steps until the 6th step:

9. *In Step 6: Configure Security Group* – the firewall rules for the instance can be configured. The SSH rule added by the system should be active, do not remove it. Add the following additional rules:
   - Allow **HTTP** traffic on port **80**.
   - Allow **HTTPS** traffic on port **443**.
   - Allow **TCP** port **8881**.
   - Allow **ICMP** protocol – all traffic.
   - Allow **TCP** ports from **42000 to 42009**.
   - Allow **UDP** ports from **42010 to 42019**.

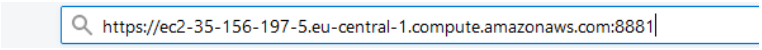
| Type | Protocol | Port Range | Source | | Description |
|---|---|---|---|---|---|
| SSH | TCP | 22 | Custom | 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| HTTPS | TCP | 443 | Custom | 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |
| Custom TCP F | TCP | 8881 | Custom | 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| All ICMP - IPv | ICMP | 0 - 65535 | Custom | 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| Custom TCP F | TCP | 42000-42009 | Custom | 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| Custom UDP I | UDP | 42010-42019 | Custom | 0.0.0.0/0 | e.g. SSH for Admin Desktop |

10. Review and launch the instance. (Note: you can create a new key pair or select an existing one if available in your account. This key is necessary for SSH login to your instance if needed.)

11. View your instances (left menu, *Instances*), wait a while (instance initializing). Then, choose the instance and look below the table at the *Description*. Find Public DNS or IP and copy it to the clipboard.




12. To access the WebAccess/VPN installation wizard, paste the IP address of your instance into your browser address bar, add **https:**// to the start of the address and port **:8881** to the end. Example:
    **https://IP-OR-DNS-OF-YOUR-INSTANCE:8881**




    HTTPS explicit is necessary since HTTP is not redirected. Ignore the invalid certificate authority notice and continue to the site (CA will be configured in the first step of installation).

13. Continue in the wizard, go to 2.5

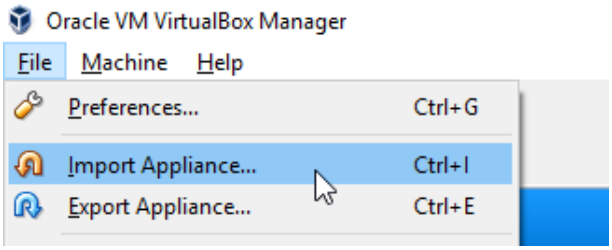
## 2.3 On-Premises Installation – VirtualBox

Both Dispatch Server and Customer Server installed on-premises as VirtualBox appliances. The provided appliance uses Ubuntu 20.04 LTS operating system and contains the installer of WebAccess/VPN. Since this is the on-premises version, the sole customer is responsible for the run of the WebAccess/VPN system, its security, and updates, including the operating system provided in the appliance.

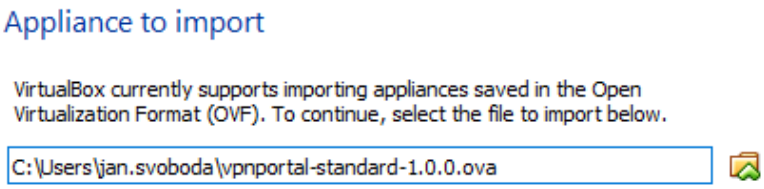
**Prerequisites:**

- **A computer with Internet access and VirtualBox installed.**
- **WebAccess/VPN .ova file** (VirtualBox appliance).
- **Domain name** for your WebAccess/VPN installation is needed. Suppose your instance has a public IP address (guaranteed for instances running in the Amazon cloud). In that case, Advantech can provide and manage a domain name for you automatically (ending with ".vpnportal.cloud" suffix).
- Recommended: A DHCP server in the network that will lease a fixed IP address to your bridged VirtualBox machine with WebAccess/VPN.

1. In your VirtualBox Manager, go to *File – Import Appliance...*



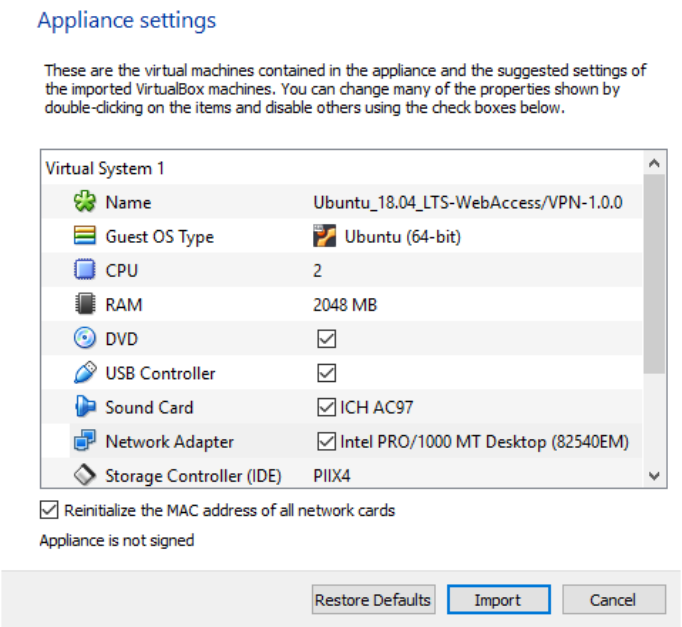

2. Choose the WebAccess-VPN .ova file to import:



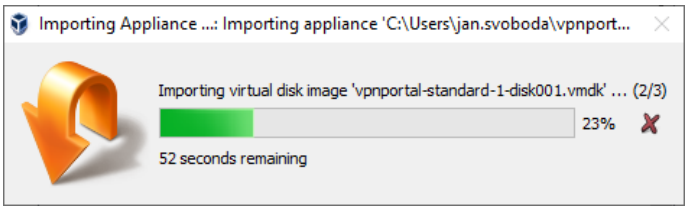
3. Review the imported settings. Recommended parameters:

   - CPU: 2
   - RAM: 2 GB
   - VideoRAM (display): 64 MB (accessible later in settings)
   - Network: bridged (accessible later in settings)
   - HDD storage size: 20 GB (accessible later in settings)

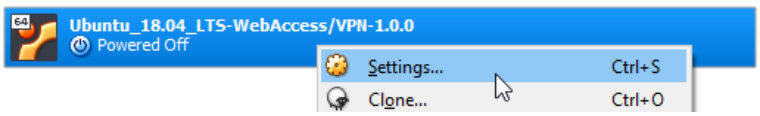
   Check the *Reinitialize the MAC address of all network cards* option. Run Import.



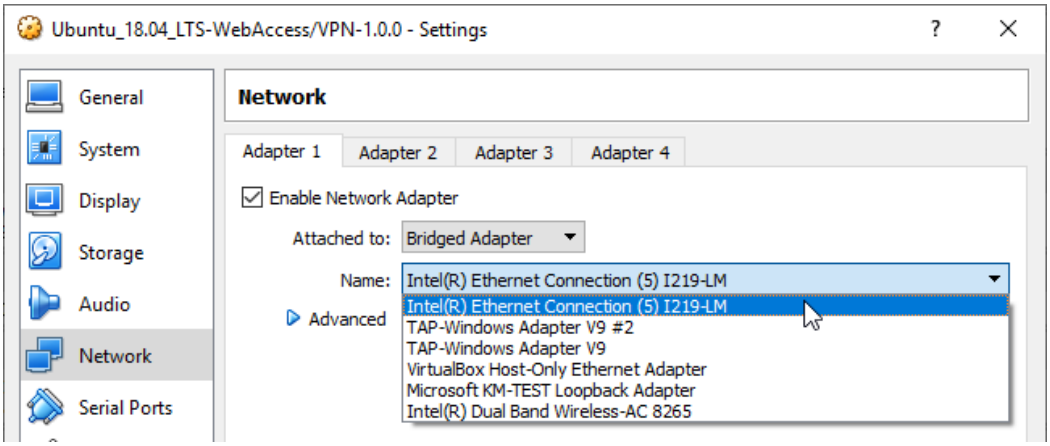

4. Wait while the appliance file is imported.




5. After the import, do not run the appliance immediately, but go to Settings and check the Network settings:

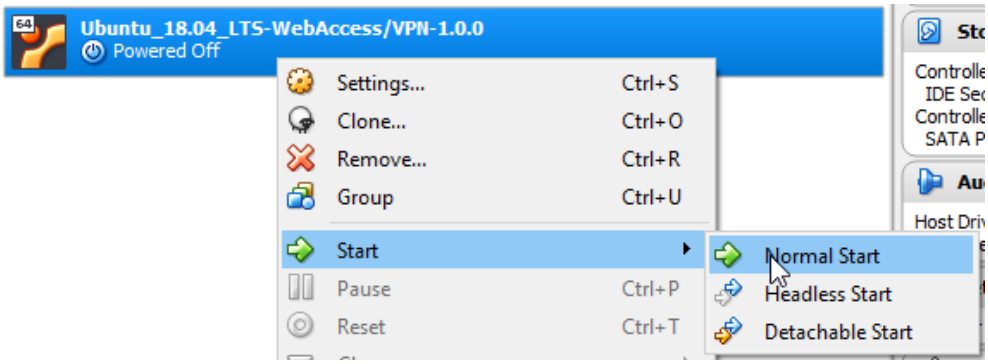


6. In Network Settings check that there is the *Bridged Adapter* set in *"Attached to:"* option. Choose your physical network interface below.



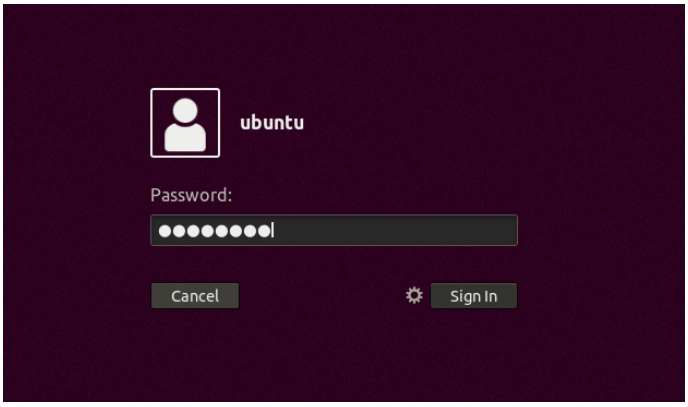

The bridged network is needed, so the WebAccess/VPN is available directly in your network. The IP address of the WebAccess/VPN has to be accessible to routers and clients you want to add to WebAccess/VPN.

7. Now run the appliance:



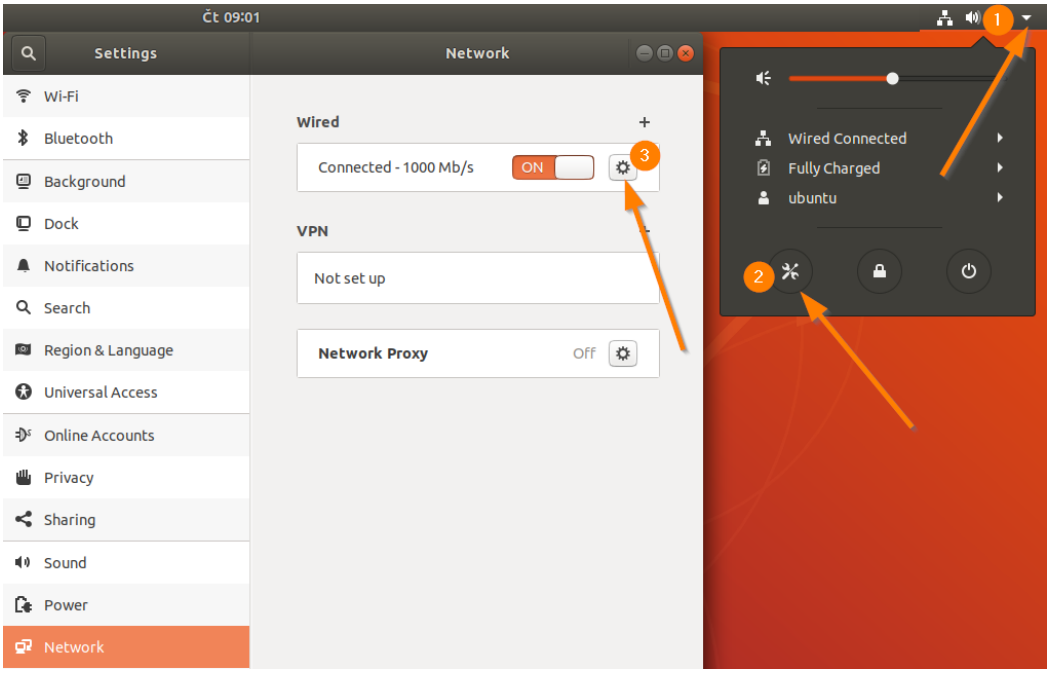
8. Wait for the system to boot and login to Ubuntu with these credentials:

   - Username: **ubuntu**
   - Password: **wavpn123**

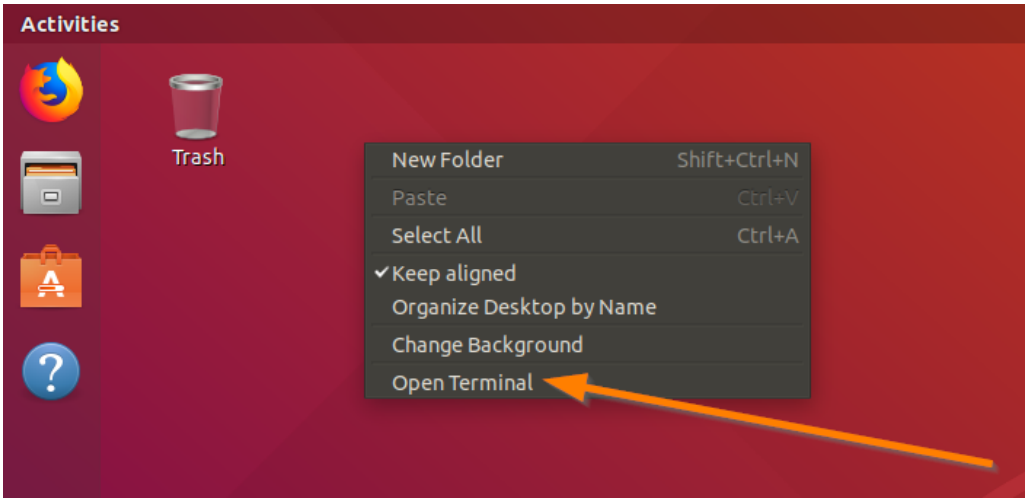


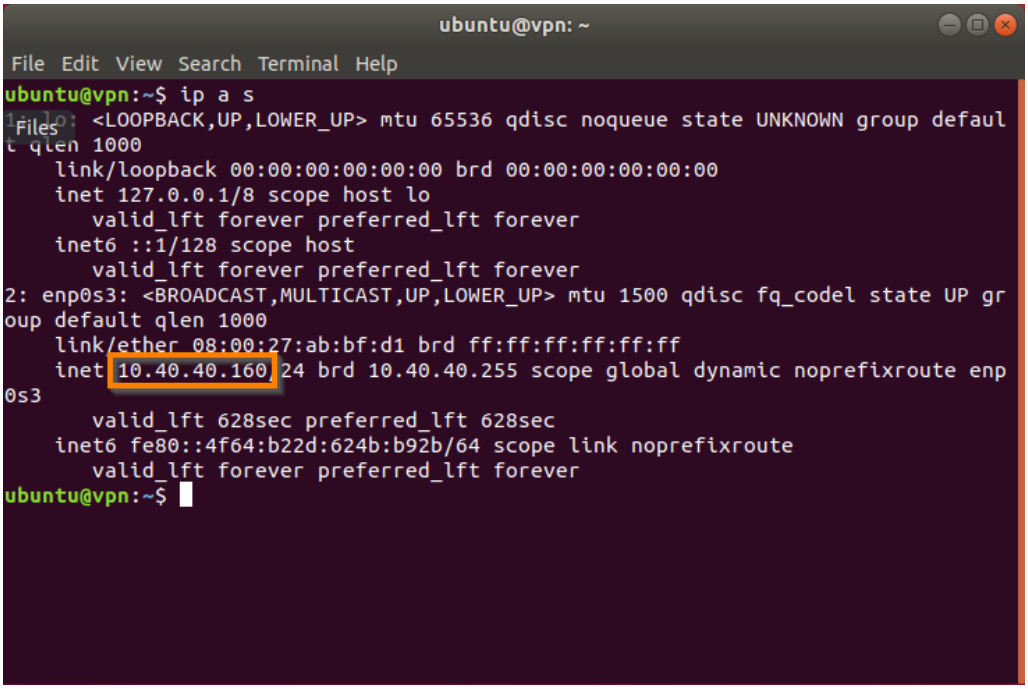

9. Find out the IP address of the appliance's bridged network interface. It is accessible via GUI in system settings or the terminal after a command prompt. Both methods are described below:

   **In GUI system settings:** Open Settings by clicking the top bar in the top right corner (1 in Figure below), choose settings icon (2), and then Network settings in the menu. Click the settings icon (3) and read the IP address in *IPv4 Address* field.



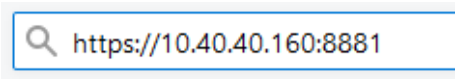
**Via terminal:** Run the terminal – right click on desktop and choose *Open Terminal*. Then use one of the commands "`ip a s`" or "`ifconfig`" to find out the IP address of physical interface (enp0s3).



10. Now go to your browser in the superior system (where VirtualBox is running) or anywhere in the network where the IP address of the appliance is accessible.

    Access the WebAccess/VPN installation wizard – type explicit **https:**// to the browser address bar, the IP address of the appliance, and port 8881. Example: **https://IP-OF-APPLIANCE:8881**

    HTTPS explicit is necessary since HTTP is not redirected. Ignore the invalid certificate authority notice and continue to the site (CA will be configured in the first step of installation).

11. Continue in the wizard, go to 2.5

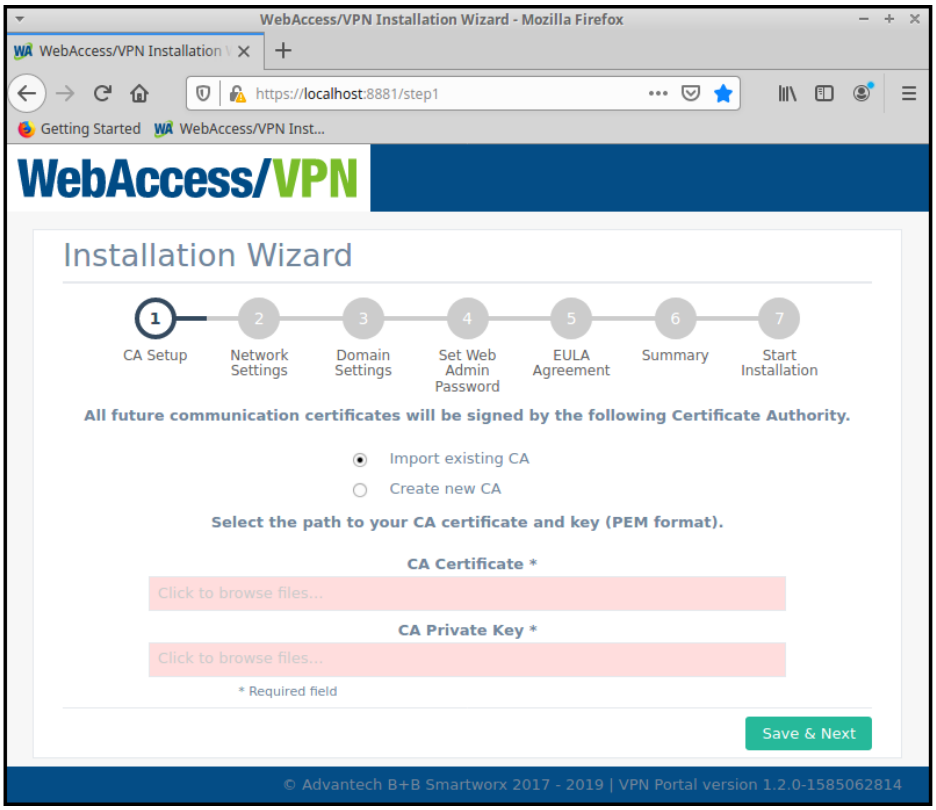
## 2.4 VPN-BOX-UNO Installation

The license file is stored in the *Desktop* folder of the *VPN-BOX-UNO23* device.

The *VPN-BOX-UNO23* product is an Advantech Embedded Automation Computer UNO-2372G with pre-installed *WebAccess/VPN* software. This device acts as the *WebAccess/VPN* server. Linux distribution based on the *Ubuntu 20.04 LTS* is installed on this computer.

Do not upgrade the Linux distribution to a newer version than 20.04 LTS; since the *WebAccess/VPN* software does not support it.

1. Connect the *VPN-BOX-UNO23* to all peripherals and the power supply; see the printed *Start Guide* for details.
2. When the device boots up, the login screen should appear. Log in as the **ubuntu** user with password **wavpn123**.
3. Open the *Mozilla Firefox* web browser by clicking the icon on the left panel.
4. The first page of the *WebAccess/VPN* Installation Wizard should pop up. If not, enter the `https://localhost:8881` address.



> Should you encounter the *Potential Security Risk Ahead* warning while accessing the web interface, proceed by selecting *Advanced...* and then *Accept the Risk and Continue*. This action is necessary to bypass the security warning and access the application interface.

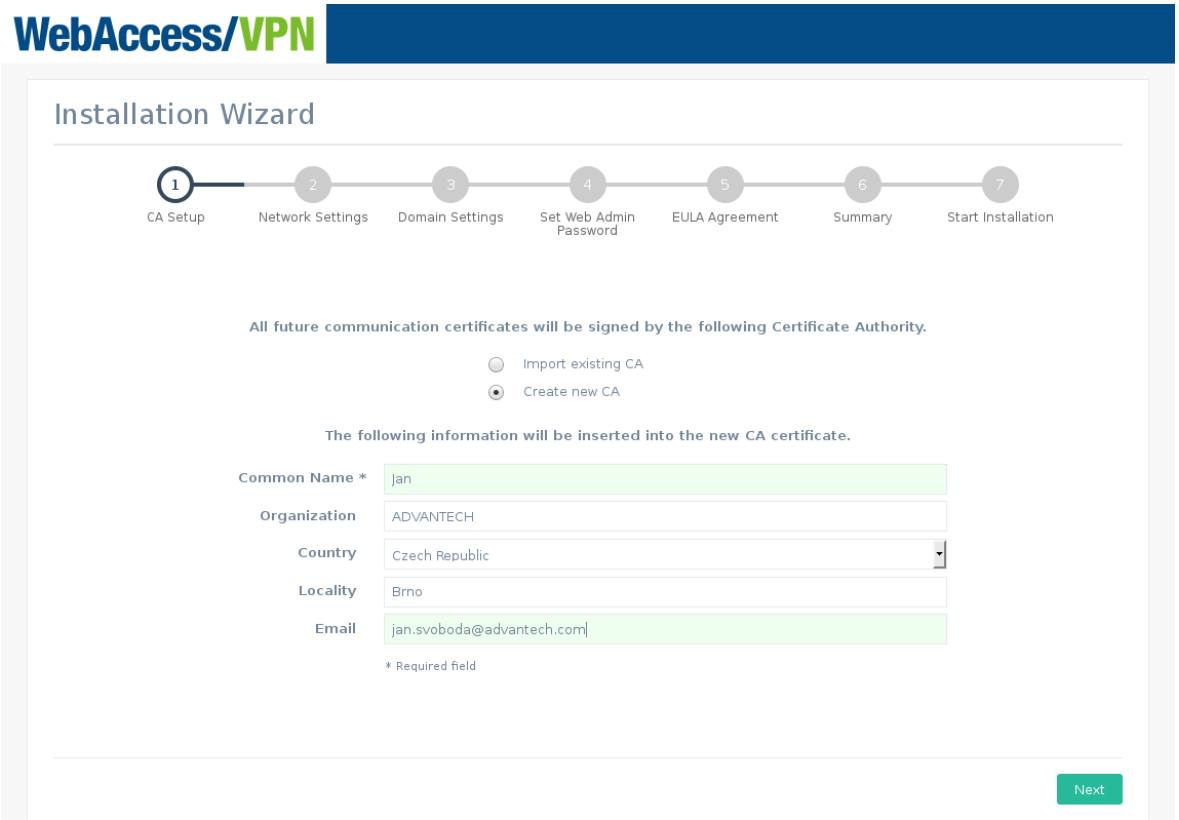
5. Continue with the configuration in the wizard, see Chapter 2.5.

The maximum overall throughput (all active VPN connections from the routers and standalone VPN clients together at one moment) of the WebAcces/VPN server installed on the UNO-2372G industrial computer is approximately 85 Mbps for both licenses (*VPN-BOX-UNO23-100* and *VPN-BOX-UNO23-500*).

## 2.5 Installation Wizard

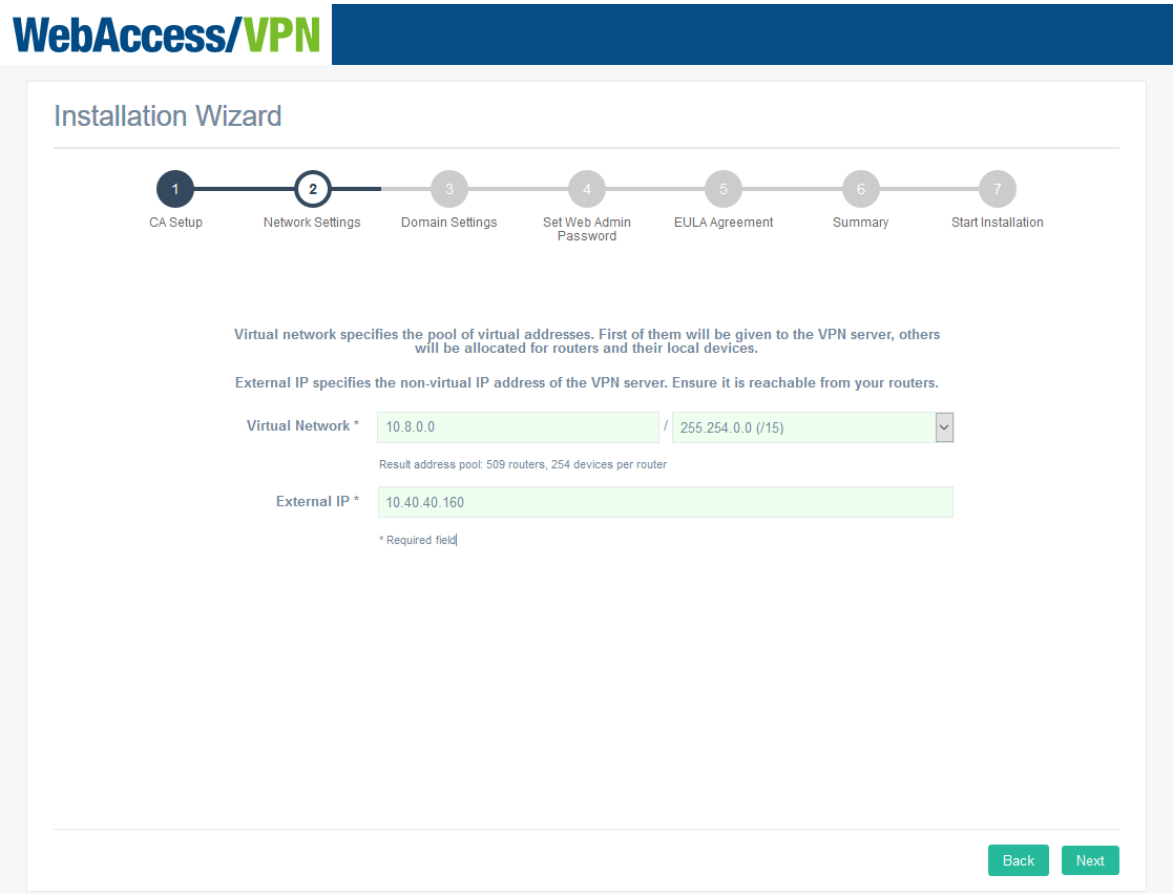
1. Follow the instructions in the installation wizard. If you don't have the Certification Authority to import (certificate file in CRT format and key file in PEM format), use the wizard to create these for you.

   **Attention:** If using your own Certificate Authority, the key file to be imported must not be password-protected!

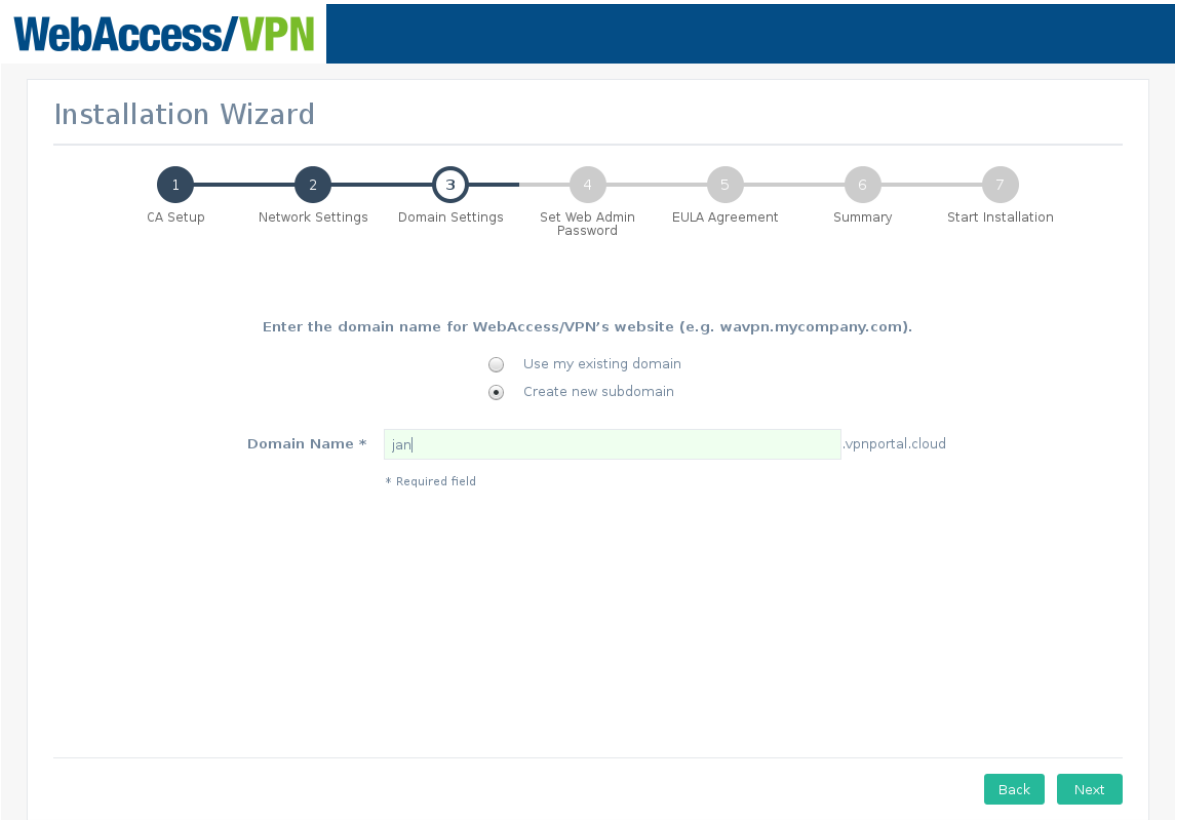


2. In Step 2, your virtual internal network is set (for OpenVPN with routers). The recommended values are network 10.8.0.0 and a mask prefix chosen from the options available. The mask will affect the number of devices possible to connect to WebAccess/VPN. See the number of routers calculated under the form field. The number of devices per router is always 254 and can not be changed. Virtual network address and mask (affecting the overall number of devices) can be changed later in the setting, but only if there are no validated routers.

   External IP is either the IP address of the Amazon instance (detected automatically, can not be changed when installing from Amazon image) or the IP address of the VirtualBox appliance.



3. In Step 3, either enter your own domain name of WebAccess/VPN (recommended for on-premises installations) or create a new subdomain managed by Advantech (available for public IP only, it is a vpnportal.cloud subdomain).



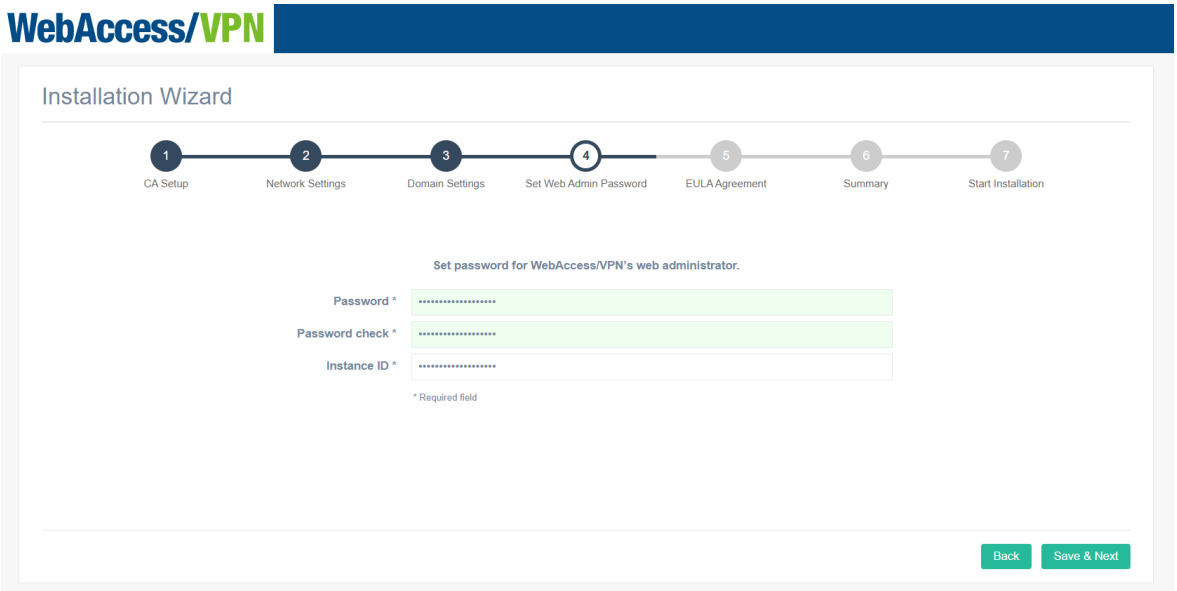

**Warning:** On AWS, do not use your instance DNS domain name (e. g. ec2-35-156-197-5.eu-central-1.compute.amazonaws.com).

Note that the AWS instance may change its public IP when stopped and run again, so either does not stop the instance or buy a fixed public IP from Amazon.

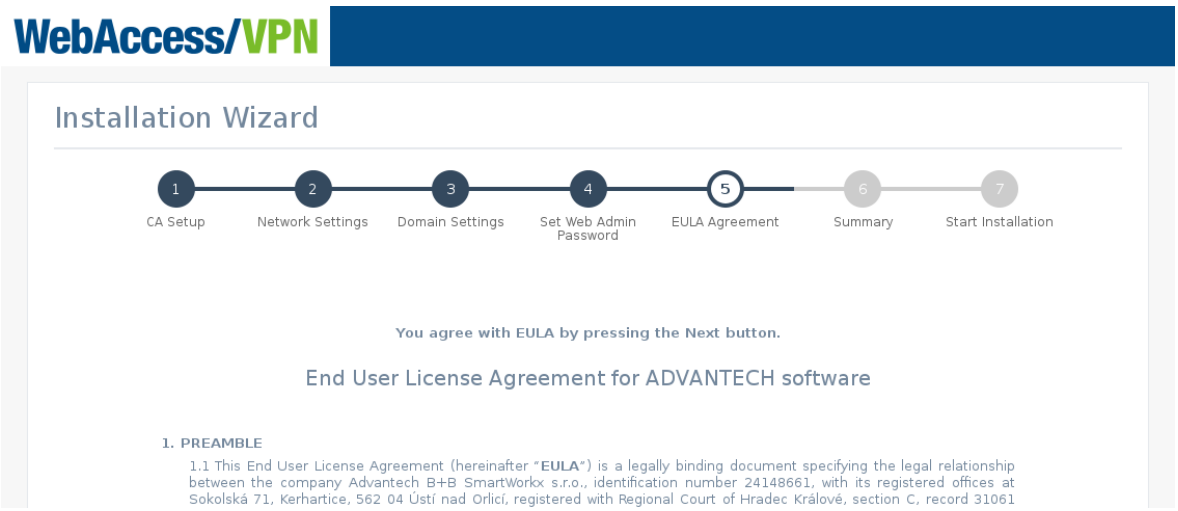
**Using your own domain name**: when directing your domain's DNS records to the IP of your installation, add this additional "A" record to your domain: ***.mydomain.com** (or *.sub.mydomain.com if your installation will use a subdomain).
This matches all possible subdomains and is necessary for some features of WebAccess/VPN.

**Using a domain name from Advantech**: Suitable for AWS. For on-premises only if your VirtualBox appliance has a public IP! Choose an unused subdomain name on domain vpnportal.cloud. The form field will go red if the name typed in is already taken. Note that Advantech will set the DNS records and manage them for you. Thus future changes are not as flexible as they would be with your domain.

4. In step 4, setup the password and fill up your instance ID from the EC2 console for Web user admin access.




5. In step 5, read and agree with the EULA:

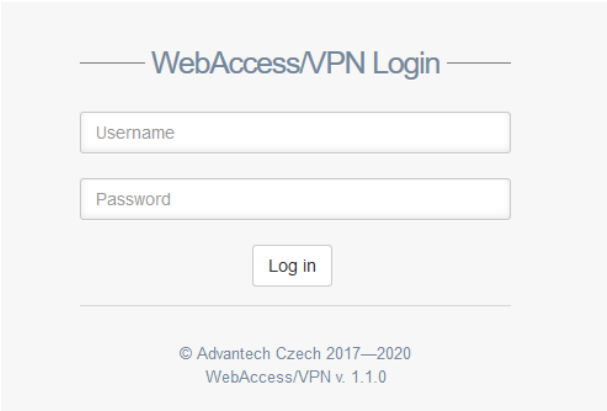


6. In step 6, check the installation parameters.

> Note that the installation wizard can be run only once and will be deactivated after the installation.

7. Click *Start installation*. There will be a progress bar showing the status of the installation. After the installation, the message "Installation is completed, you can continue to login" will appear and the button *Go to Login* will be active.

8. Click that button, or go to page **https://IP-OR-DOMAIN-OF-INSTANCE-OR-APPLIANCE** and login to your WebAccess/VPN admin account (username **admin**, and password you set in wizard). The installation wizard is now deactivated.




The default license described in Chapter 1.3 is active after installation. You can download router apps for the next step from WebAccess/VPN. See Chapter 4.8.1.

## 2.6 Performance Scaling Recommendations

These are the results of hardware tests from which the following recommendations emerged.

### 2.6.1 Amazon Instance Type

We recommend choosing an instance with at least 2 CPUs and 4 GB of RAM for production use. So "t2.medium" or a higher AWS instance type is recommended. Also, see the findings and recommendations below which emerged from the standalone hardware test.

### 2.6.2 Standalone Hardware

A standalone hardware test was carried out. See the test description and results in appendix A. The following findings and recommendations emerged from the test:

- This test shows a total throughput cap of around 200 Mbps for an Intel Xeon E3-1245 v5 CPU. As the primary limitation for OpenVPN is CPU, using a stronger CPU would probably lead to a higher cap. The overall number of devices does not affect throughput significantly. (It does not matter how many devices you have. The overall traffic is what counts – e.g., 1000 devices, each with 20 kbps traffic, would produce 20 Mbps of overall traffic.)
- Currently, OpenVPN is not capable of using more than 1 CPU core, so more CPU cores do not help with traffic in this case. Thus 2 CPU cores will be sufficient for most applications (1 for OpenVPN and 1 for the rest).

## 2.7 Security Update Patch for Frontend

This update patches up all known security vulnerabilities in the Frontend component of WebAccess/VPN.

Note that this security patch is applicable to 1.1.x versions of WebAccess/VPN installations.

For implementation of this patch do the following steps:

Login to WebAccess/VPN system (Ubuntu on standalone VirtualBox / AWS / UNO PC installation, may be via SSH).

In terminal, run the following:

- To download the patch: `curl https://icr.advantech.com/support/router-models/download/1036/patch-wavpn.tar.gz\ --output patch-wavpn.tar.gz`
- To extract the patch: `tar -xzvf patch-wavpn.tar.gz`
- Go to the extracted directory: `cd patch-wavpn`
- Run the patch script: `sudo ./patch-wavpn.sh`
- Provide **password** when prompted.
- The script will inform you in console about the progress.

The script will patch these CVEs (provided link to explanation and code changes applied):

*CVE-2019-10910:* https://symfony.com/blog/cve-2019-10910
*CVE-2019-10911:* https://symfony.com/blog/cve-2019-10911
*CVE-2019-10912:* https://symfony.com/blog/cve-2019-10912
*CVE-2019-10913:* https://symfony.com/blog/cve-2019-10913
*CVE-2019-18887:* https://symfony.com/blog/cve-2019-18887
*CVE-2019-18888:* https://symfony.com/blog/cve-2019-18888
*CVE-2019-18889:* https://symfony.com/blog/cve-2019-18889

# 3. Configuration of Advantech Router

> Firmware version 6.2.1 or higher is required in the router for *WebAccess/VPN* to work properly!

## 3.1 Upload Router App (User Module) VPN Portal

Upload the router app *VPN Portal* to the router to connect the router to *WebAccess/VPN*. It can be done on the *Router Apps* page in the router's Web interface.

> The *VPN Portal* router app is not a part of the router's firmware. It can be downloaded from within WebAccess/VPN – see Chapter 4.8.1 or from icr.advantech.com. The installation process for a router app is described in the Configuration Manual (see [1, 2, 3 or 4]). The router app is compatible with both v2 and v3 routers.

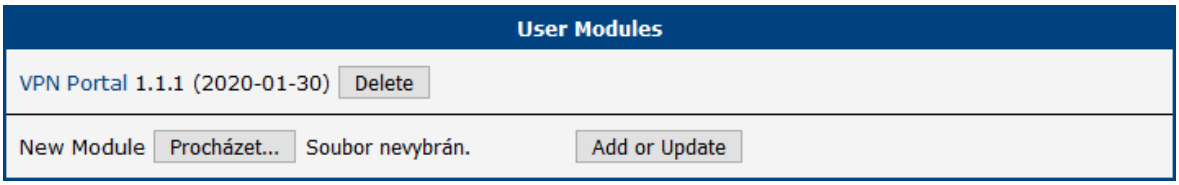



Figure 3: Router App *VPN Portal* after upload to the router

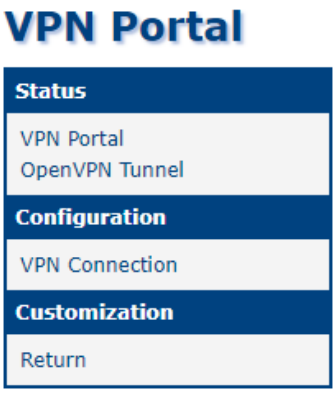



Figure 4: Router app menu

The Web interface of the router app is accessible by clicking on the router app's name. The user module menu is on the left. The *VPN Portal Status* section is the landing page. On the pages in the *Status* section, you can see the status messages regarding the connection with WebAccess/VPN and the OpenVPN tunnel establishment (taken from the *System Log* of the router). In the *Configuration* section there is the *VPN Connection* page with configuration parameters. You can return to the router's Web interface using the *Return* button in the *Customization* section.

## 3.2 Connect the Router to WebAccess/VPN

Make sure that the WAN is configured in the router, so it is possible to ping the Dispatch Server (Internet) through the WAN interface. Set the IP address or URL of the Dispatch Server on the *VPN Connection* configuration page. Ensure that the *Enable* box is checked, and click the *Apply* button.

> In most cases the DS is installed on the same server as CS (e.g., customer-managed installations in the cloud), so fill in your WebAccess/VPN IP address or domain name into *Primary Local DS* field. Secondary and Tertiary DS fields are not mandatory.

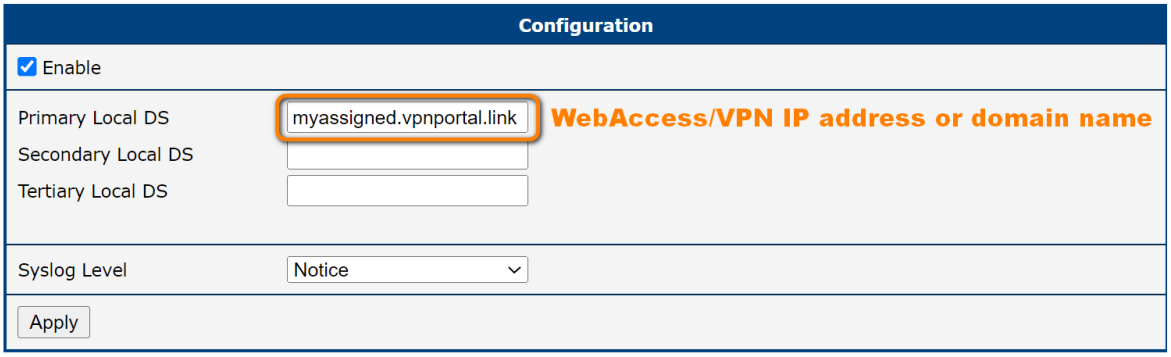



Figure 5: *VPN Connection* configuration page – Dispatch Server IP

Three Dispatch Servers can be configured: *Primary*, *Secondary* and *Tertiary Local DS*. The router tries to connect to the *Primary Local DS* first. If not successful, it tries to connect to the *Secondary Local DS*. If not successful, it tries *Tertiary Local DS*. This configuration allows running a backup Dispatch Server in case of Dispatch Server maintenance. Both URLs and IP addresses can be used in the DS configuration fields.

## 3.3 Validate the Router on WebAccess/VPN

Login to *WebAccess/VPN* Web UI and validate the router as shown in Figure 6:

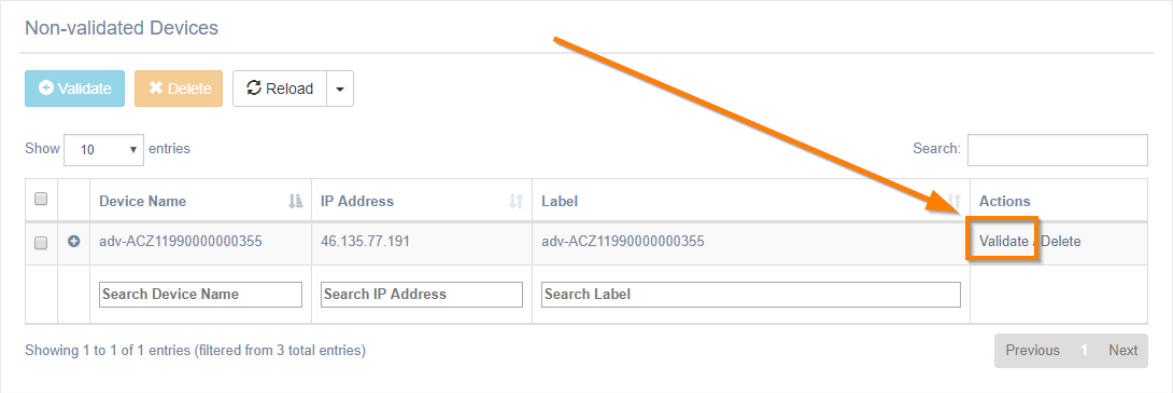
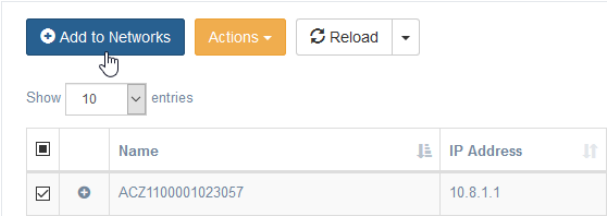



Figure 6: Validating the router in WebAccess/VPN Web UI

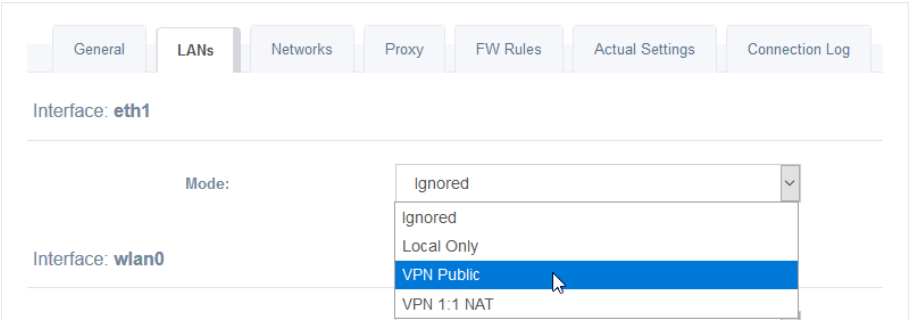
## 3.4 Set the Router Access Policy

> By validating routers to WebAccess/VPN, they do not see each other automatically.

The Routers have to be added into a Network to see each other in the VPN tunnel.




Devices connected to the Router can access the VPN tunnel only after the Router LAN interface is set to one of the VPN modes – go to *Router*, *Edit*, *LANs*. For more see Chapter 4.



## 3.5 Router App (User Module) Status and Log Messages

After the router is validated in WebAccess/VPN Web UI, you can see the "`Ready for incoming messages`" notice on *VPN Portal* status page in the router:

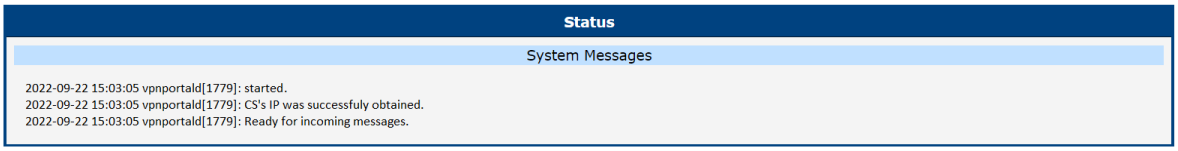



Figure 7: *VPN Portal* status page of the validated router

Also on the *OpenVPN Tunnel* page there will be "`Initialization Sequence Completed`" notice if the tunnel establishment is successful:

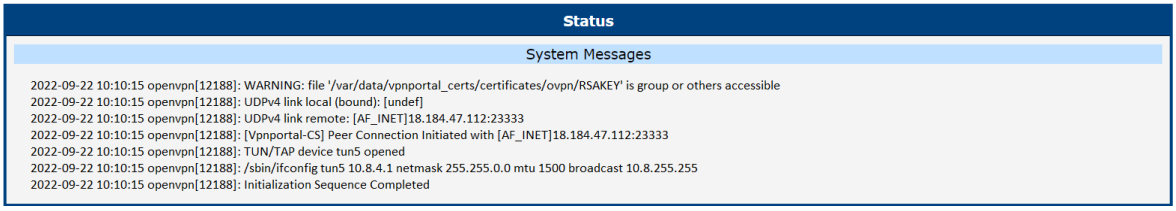



Figure 8: *OpenVPN Tunnel* status page of the validated router

If you return to the router's Web interface, you can verify that there is a new tunnel network interface created and that Route Table has changed accordingly:

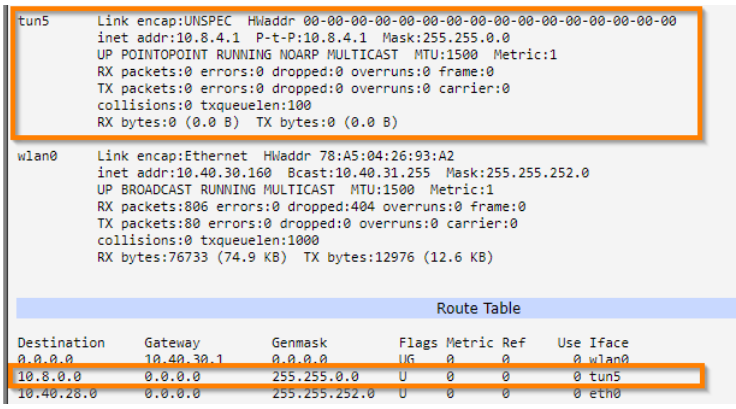



Figure 9: Example of a new tunnel network interface and Route Table

Now you can use the WebAccess/VPN Web UI to create new networks, modify router LANs and place them into the previously created networks to make them visible to each other. In addition, for the routers that share at least one network, it should be possible to ping between devices in their (VPN Public or NATted) LANs and between each router.

### 3.5.1 Router App (User Module) Log Messages

The router app starts automatically after the router is turned on (if enabled previously). The router attempts to obtain the Customer Server's IP address from the Dispatch Server (DS). There are 3 possible outcomes:

- *"Failed to connect to the Dispatch Server."* – The dispatch server is unreachable or stopped.
- *"CS's IP was successfully obtained."* – The router app received the necessary address, and now it can move to the next phase.

If the router obtains the Customer Server's (CS) IP address, it will contact the CS to ask to be allowed into the WebAccess/VPN network. There are 3 possible outcomes:

- *"Failed to connect to the Customer Server."* – The Customer Server is unreachable or stopped.
- *"Negative response to a request for OVPN certificates."* – The router hasn't been validated on the Customer Server yet.
- *"Ready for incoming messages"* – Tunnel between router and Customer Server has been established. Therefore, a ping to the CS's virtual IP address (10.8.0.1) should be possible.

# 4. WebAccess/VPN User Interface

## 4.1 Login to WebAccess/VPN

WebAccess/VPN (CS) 's Web user interface runs on the server after the installation. Navigate your browser to the server and login:

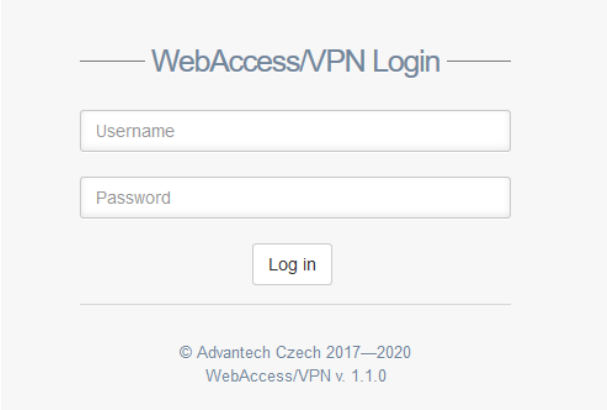



Figure 10: Login to WebAccess/VPN

## 4.2 Dashboard

After login to WebAccess/VPN, the Dashboard will show as the landing page:

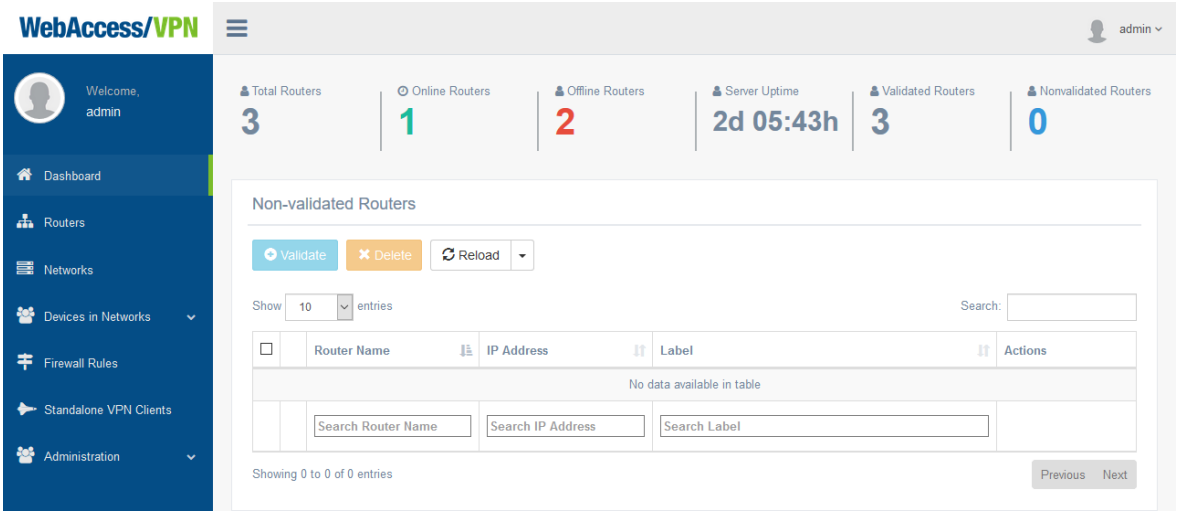



Figure 11: WebAccess/VPN Dashboard

An overview and basic statistics can be found at the top of the Dashboard: Number of *Total Routers* in WebAccess/VPN, *Online Routers*, *Offline Routers*, *Server Uptime*, *Validated Routers* and *Non-validated Routers*.

The list of Non-validated routers is below the overview. Validate connected routers as shown in Figure 6. You can also delete routers you do not want to validate. You can do these actions in bulk using the checkboxes and buttons at the top of the devices list. This is the only place (on the Dashboard) you can validate the routers manually in WebAccess/VPN. There is also automatic option – pre-validation – see Chapter 4.8.2.

> By validating routers to WebAccess/VPN, they do not see each other automatically. The routers have to be added to a network, and its LAN interface (Routers – Edit) has to be set to one of the VPN modes.

There is a WebAccess/VPN main menu on the left. All the menu items are described in the following sections.

## 4.3 Routers

A table of all validated routers can be found in the *Routers* section of WebAccess/VPN. With buttons at the top, you can add the router to a network in bulk (*Add to Networks*), disable/enable access to the VPN tunnel, and delete the routers (*Actions* dropdown button). You can reload the page or turn on the autorefresh of the page (after 5, 10, or 30 seconds) when you drop down the *Reload* button. Router properties are explained in Table 1 below.

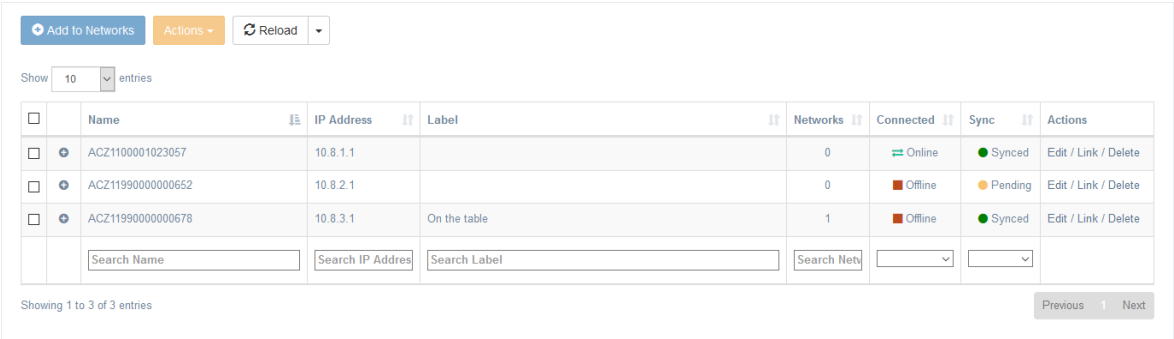



Figure 12: Routers in WebAccess/VPN

| Router Property | Description |
|---|---|
| Name | An automatically obtained name of the Router. Based on Serial Number in most cases (if SN is unavailable, based on MAC address, or a random number). It can be changed on *General* tab after click on *Edit* action. |
| IP Address | The IP address of the Router's end of the OpenVPN tunnel. |
| Label | The editable label of the device. It can be changed on *General* tab after click on *Edit* action. |
| Networks | The number of networks the device is added to. See section 4.5. |
| Connected | **Online** (green arrows) – connected to WebAccess/VPN.<br>**Offline** (red square) – not connected to WebAccess/VPN.<br>**Disabled** (grey square) – not allowed to connect to WebAccess/VPN (editable either via *Actions* dropdown button or on the tab *General* in Router edit). |
| Sync | **Synced** (green) – All requested settings were applied to the Router, no pending operations.<br>**Pending** (yellow) – Some changes are not yet propagated to the Router.<br>**Failed** (red) – Some settings caused an error on the Router. Check the router app's log in the Router for details about the failure. |
| Actions | **Edit** – Access the router's main page with more information and actions available. More in section 4.3.1.<br>**Link** – Redirect to the router's login website. This can be affected by settings on *Proxy* tab in Router edit. More in section 4.3.4.<br>**Delete** – Permanently remove the Router. More in section 4.3.5. |

Table 1: Routers properties

A quick overview of the Router's details is shown when the user clicks on the plus sign before the *Name*. See Figure 13. The overview will pop up as a panel on the right with *Device Detail*, *LANs* details, *Device Networks* (networks containing the device), and *Device Statistics*. This is the same information you can view by clicking *Edit* link on the Router, but this is a shortcut – they are read-only, and no page reload is needed.

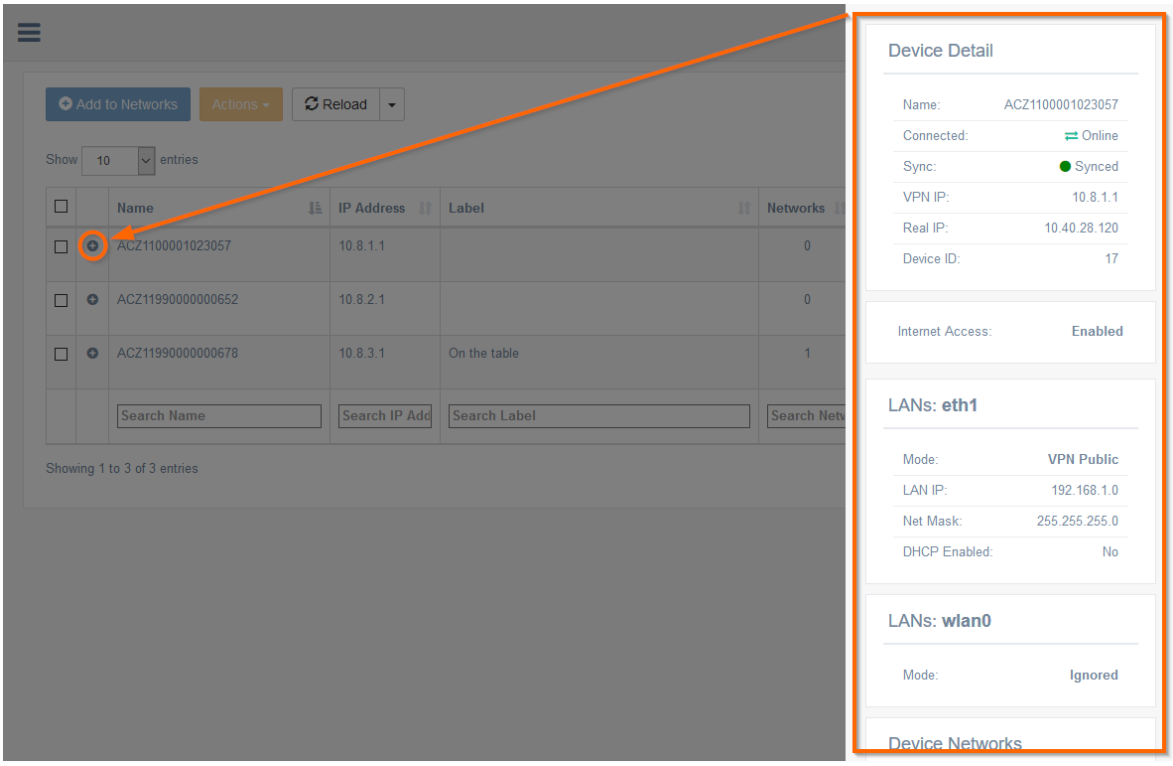



Figure 13: Routers – Overview of a Router

### 4.3.1 Routers: Edit

It is possible to control Router's general settings, LANs, Networks membership, Proxy, and Firewall and see the Actual Settings and Connection Log on this Edit page of a Router.

#### LANs Tab

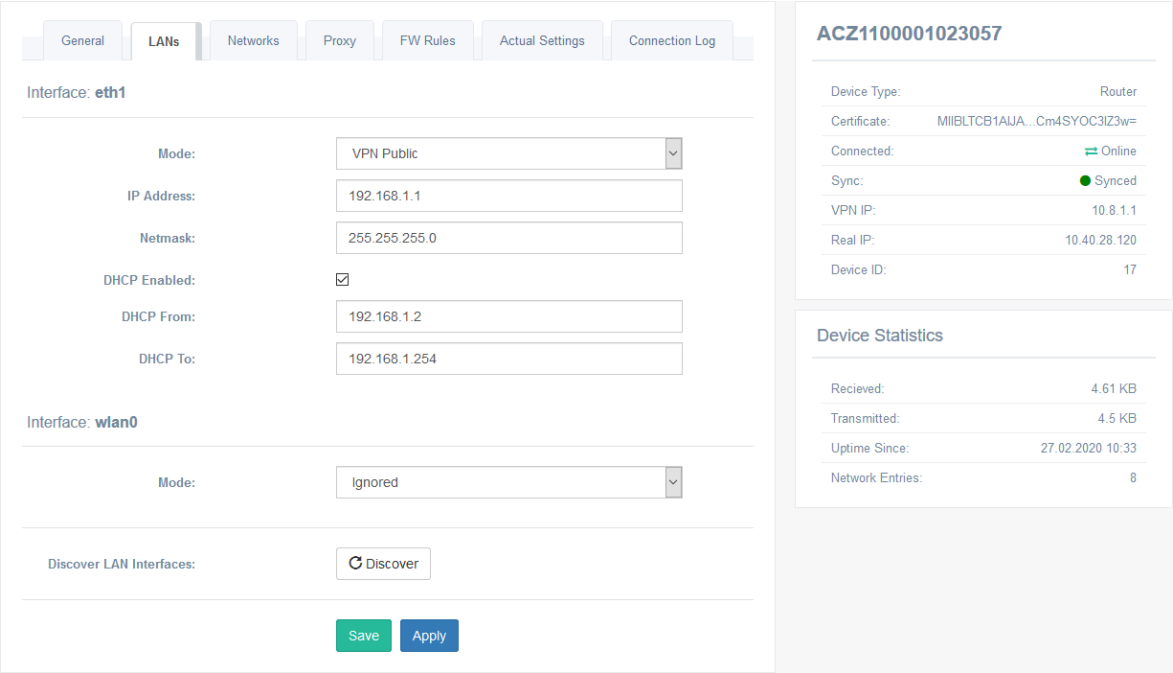



Figure 14: Routers – main page of a Router – Edit LANs

| Interface Mode | Description |
|---|---|
| Ignored | Customer Server is not managing the Router's LAN. |
| Local Only | Administrator can configure the LAN, but it is invisible for all other devices in WebAccess/VPN. The IP Address, Netmask, and DHCP can be configured. |
| VPN Public | Administrator can configure the LAN, which is visible to all Routers (and devices behind them) that share at least one network with this Router. The IP Address, Netmask and DHCP can be configured, see Figure 14 |
| VPN 1:1 NAT | LAN addresses are translated to the virtual address space so that devices within the LAN are accessible via virtual addresses (for devices that share at least one network with this one). See more in section 4.3.2. |

Table 2: Devices – LANs Interface Modes

**Interfaces** Every LAN interface of a Router can be configured, including *wlan0* and *eth2* if present in a Router. One of the modes described in the Table above can be chosen for an

interface. Both buttons *Save* and *Apply* will propagate the changes directly to the router, but the *Save* button will return you to the table of devices.

**Discover** This feature is intended for a situation where there was an interface change on the Router (e.g., Backup Routes configuration was changed on the Router), and you want to scan the interfaces again to see them updated (so you do not have to delete and validate the router again). Discover can be requested only if the Router is online.

> The *Discover* button will reset the LAN modes set to interfaces to default (Ignored). The values will be maintained, but the modes will be reset!

### General Tab

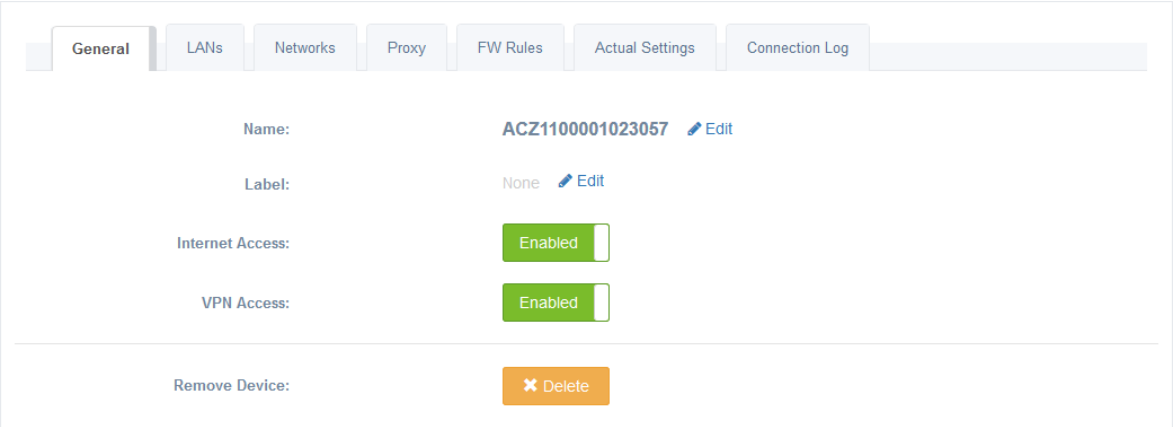



Figure 15: Routers – General tab of a Router

**Name, Label:** Rename the Router or change the Label by *Edit* link with the pencil icon.

**Internet Access:** You can disable (and enable again) the *Internet Access* for the Router using the toggle switch. This will send the request to be propagated on the Router, so the Router may go to a Pending state if it is Offline or Disabled. The actual state of the Internet Access setting propagated to the Router is shown on the *Actual Settings* tab.

**VPN Access:** The *VPN Access* for the Router can be disabled (and enabled again). This will disconnect the Router from the VPN tunnel, which can be used as a temporary ban or delete (e.g., when you want to send the router to be repaired, change in the Router's physical administration, etc.). This is the action done on the server, and it will take effect immediately. The connected status of the Router will be changed to *Disabled*.

**Remove Device:** The *Delete* button will remove the device from the WebAccess/VPN (after the confirmation dialogue). The validation process has to be repeated to add the device in the future.

### Networks Tab

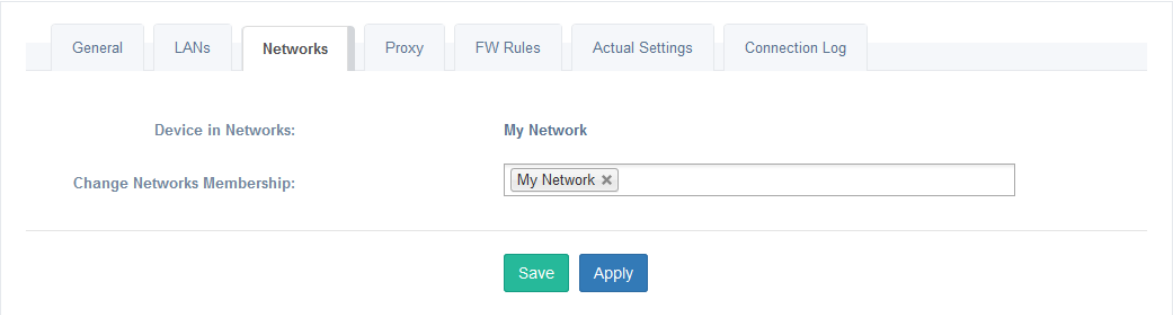



Figure 16: Routers – Networks membership of a Router

You can add a Router to one or more Networks on this tab. Both buttons *Save* and *Apply* will save the new membership, but the *Save* button will return you to the table of devices.

### Proxy Tab

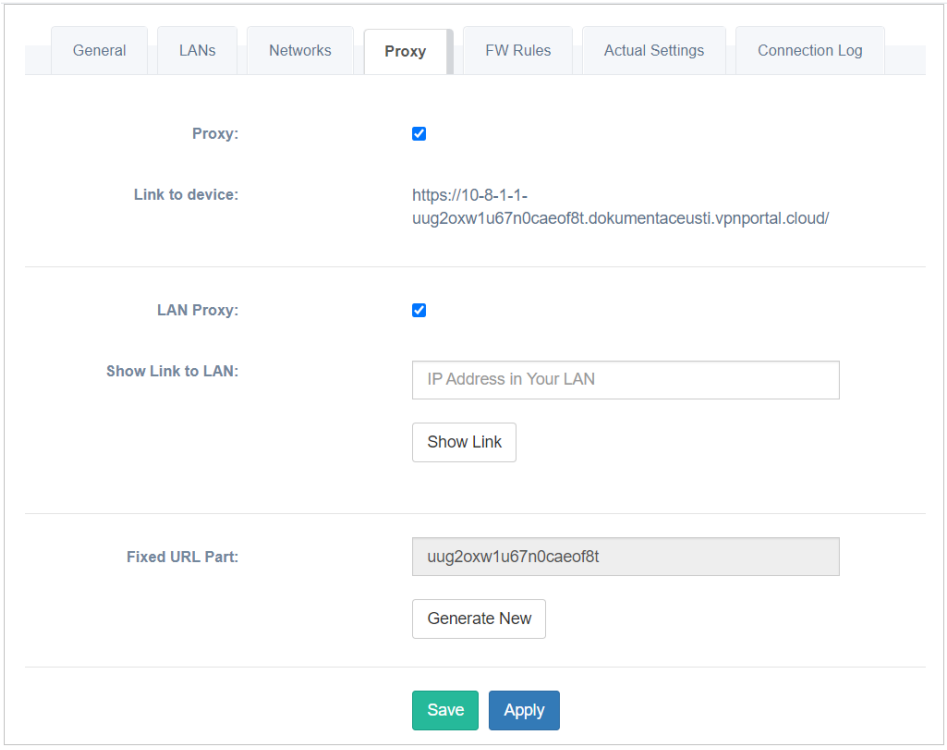



Figure 17: Routers – Proxy settings of a Router

**Proxy** Enable or disable the proxy Link to the Router (access via VPN tunnel). If enabled, the link is shown under the checkbox (the same as *Link* action in the Routers table). The default state is affected by Proxy settings in *Administration – Settings*.

**LAN Proxy** Enable or disable the proxy for devices in LANs behind the router (access via VPN tunnel). If enabled, you can use the address creator below the checkbox to see the link to your device. Fill in your device's local IP address and click *Show Link* button. LAN proxy works on both *HTTP* and *HTTPS* url.

The default state is affected by Proxy settings in *Administration – Settings*.

**Fixed URL Part** This section is visible only if one of the proxies is enabled. You can click the *Generate New* button, and all the proxy links for the Router will be re-generated. This can be used as a security reset (you have provided someone the proxy link, and when you generate a new one, his link will not work).

### FW Rules Tab

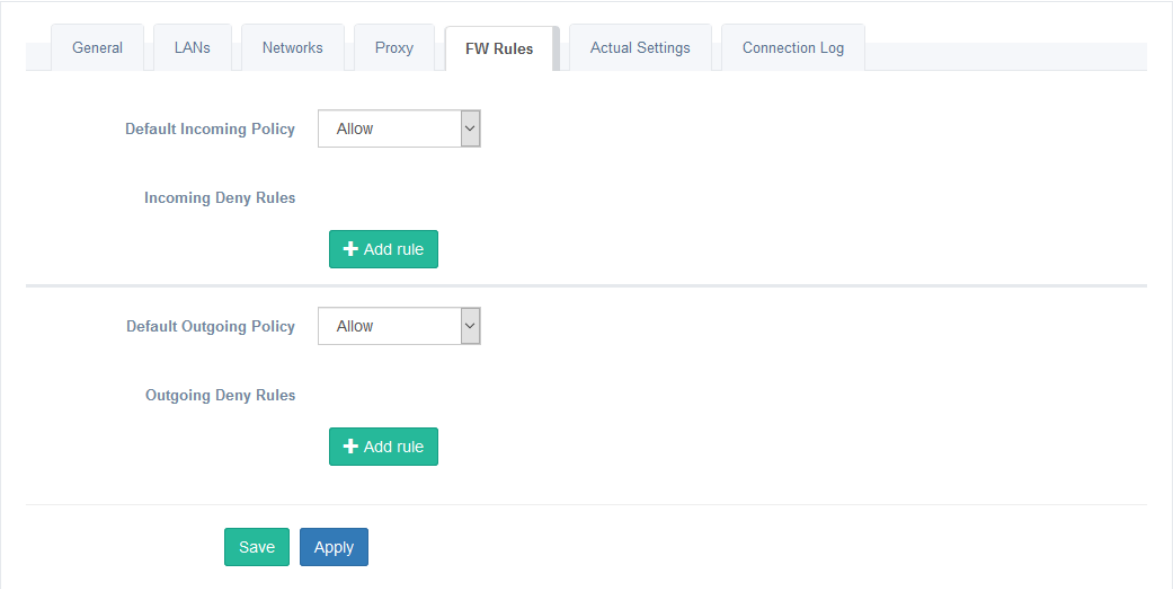



Figure 18: Routers – Firewall Rules

Custom filtering rules can be created on the *FW Rules* tab for the Router. Use the green *Add rule* button to create a rule.

See more information in section 4.3.3 below.

### Actual Settings Tab

View the settings that are already on the Router. This information could be inaccurate for the LANs in *Ignored* mode since it could be changed manually on the router.

### Connection Log Tab

View the connection logs for the Router. This is filtered overall Connection Log accessible in *Administration* – Logs.

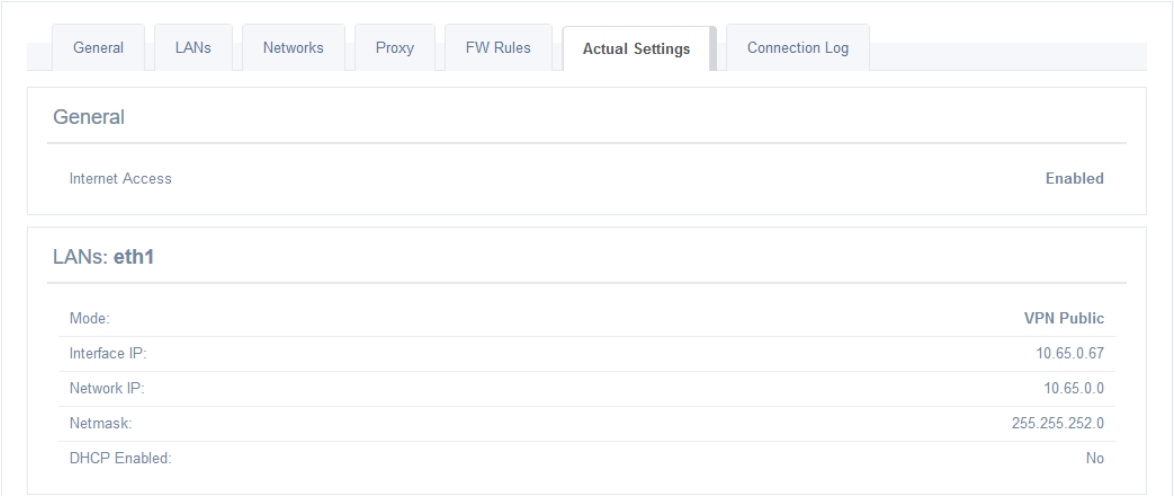



Figure 19: Routers – Actual Settings of a Router

Figure 20: Routers – Connection Log of a Router

### 4.3.2 1:1 NAT

WebAccess/VPN supports 1:1 NATting. This means that the devices in the Router's LAN would be visible in WebAccess/VPN under their assigned virtual IPs. To configure 1:1 NAT on an interface, it is necessary to choose the *VPN 1:1 NAT* interface mode and setup:

- Local Network: the pool of addresses under which the device is known locally (IP, Netmask).
- Virtual Network: the pool of addresses under which the device will be known (accessible) in the WebAccess/VPN (Virtual IP, Virtual Netmask).

See those parameters in the Figure below:

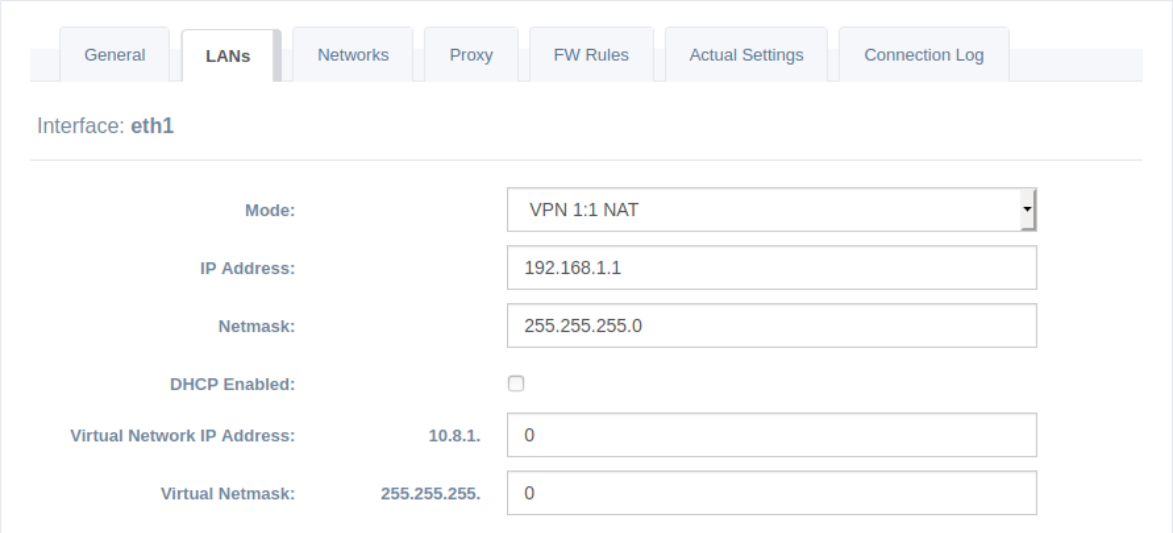



Figure 21: Routers – 1:1 NAT Interface Mode

In *VPN 1:1 NAT* mode, the Customer Server reserves a pool of 254 virtual IP addresses for each router. This amount can not be changed in the current version.

For instance, if two routers are connected to the Customer Server:

- Virtual IP of the first router is 10.8.1.1, and the pool of virtual IPs for LAN devices behind this router is: 10.8.1.2–10.8.1.254.
- Virtual IP of the second router is 10.8.2.1; the pool of virtual IPs for LAN devices behind this router is: 10.8.2.2–10.8.2.254.
- And so on...

### 1:1 NAT Example 1

- Router has LAN 192.168.15.0/24 on eth0.
- Virtual IP of the router is 10.8.2.1.
- Configuration of 1:1 NAT on eth0 is as follows:
  - (Local) *IP Address*: 192.168.15.1
  - (Local) *Netmask*: 255.255.255.0
  - *Virtual Network IP Address*: 10.8.2.0
  - *Virtual Netmask*: 255.255.255.0

In this case, the router translates the local network to the virtual network. This means that the client, e.g. with IP 192.168.15.10, will be visible under 10.8.2.10 virtual IP (and so on ...).

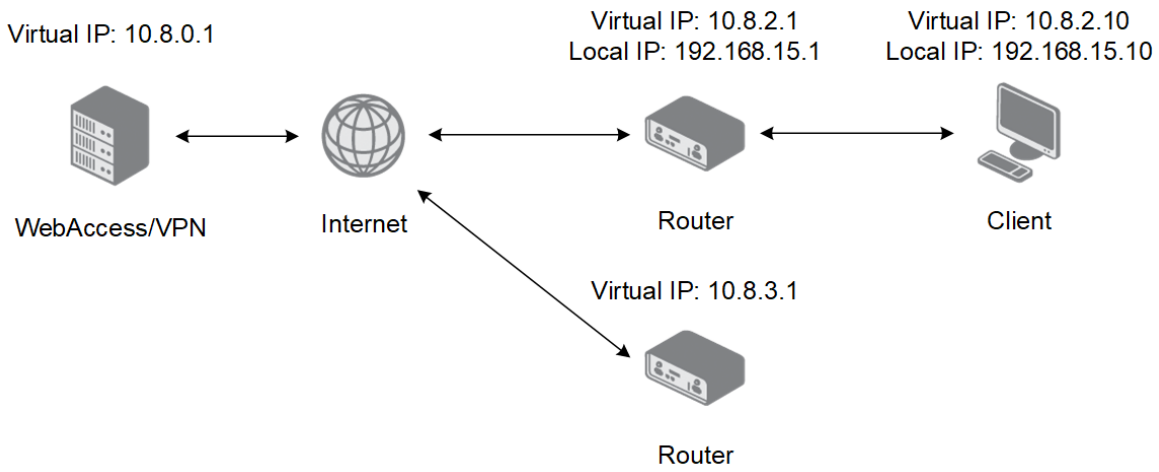



Figure 22: 1:1 NAT Example 1

### 1:1 NAT Example 2

More than one 1:1 NATs can be configured for one device. In this case, all such LANs must be subnetted to fit within the virtual address range reserved for the router.

- Router has LAN 192.168.15.0/25 on eth0 and 192.168.15.128/25 on eth1.
- Virtual IP of the router is 10.8.2.1 (eth0)
- Configuration of 1:1 NAT on eth0 is as follows:
  - (Local) *IP Address*: 192.168.15.1
  - (Local) *Netmask*: 255.255.255.128
  - *Virtual Network IP Address*: 10.8.2.0
  - *Virtual Netmask*: 255.255.255.128

- Configuration of 1:1 NAT on eth1 is as follows:
  - (Local) *IP Address*: 192.168.15.129
  - (Local) *Netmask*: 255.255.255.128
  - *Virtual Network IP Address*: 10.8.2.128
  - *Virtual Netmask*: 255.255.255.128

This means that when somebody tries to ping 10.8.2.50 from within WebAccess/VPN, it will be delivered to a device located behind the eth0 interface with the address 192.168.15.50. Likewise, if someone tries to ping 10.8.2.130, it will be delivered to the device located behind the eth1 interface with IP address 192.168.15.130.

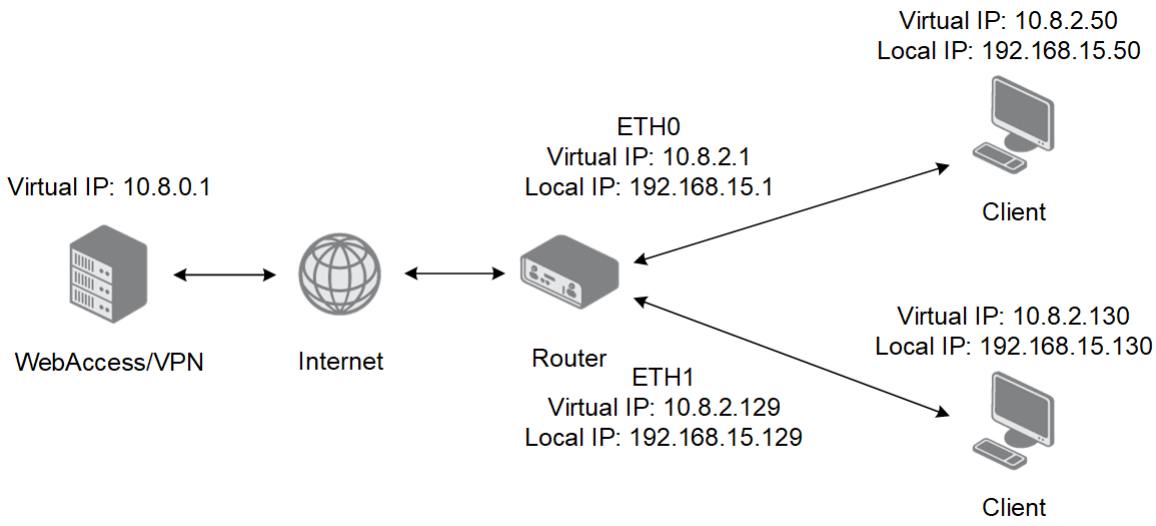



Figure 23: 1:1 NAT Example 2

The translation will work adequately if we change the local IP setting of eth1 to 192.168.16.128/25 (replaced *15* to *16*). It will even work if we change the local IP to 192.168.17.0/24 (as long as we keep the value ...128/25 for the virtual IP address). In this configuration, the addresses 10.8.2.129–10.8.2.254 will be translated to 192.168.17.129–192.168.17.254 and vice versa.

### 1:1 NAT Example 3

As in this example, networks can also be divided, so the local networks are different for every physical interface, but the virtual network is the same across the interfaces.

- Router has LAN 192.168.5.0/24 on eth0 and 192.168.10.0/24 on eth1.
- Virtual IP of the router is 10.8.3.1 (eth0)
- Configuration of 1:1 NAT on eth0 is as follows:
  - (Local) *IP Address*: 192.168.5.1

  - (Local) *Netmask*: 255.255.255.0
  - *Virtual Network IP Address*: 10.8.3.0
  - *Virtual Netmask*: 255.255.255.128

- Configuration of 1:1 NAT on eth1 is as follows:
  - (Local) *IP Address*: 192.168.10.1
  - (Local) *Netmask*: 255.255.255.0
  - *Virtual Network IP Address*: 10.8.3.128
  - *Virtual Netmask*: 255.255.255.128

The translations then will be as follows:
10.8.3.2 to 192.168.5.2,
10.8.3.3 to 192.168.5.3,
10.8.3.129 to 192.168.10.1,
10.8.3.130 to 192.168.10.2,
etc.

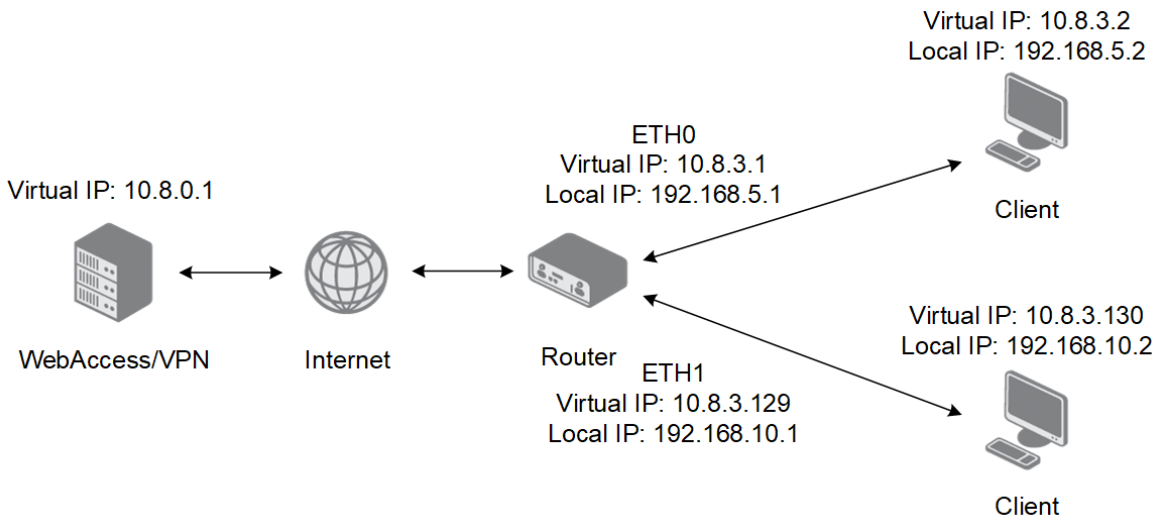



Figure 24: 1:1 NAT Example 3

### 4.3.3 Firewall Rules for Router

> Router/Standalone VPN Client firewall is part of WebAccess/VPN, and these rules are not propagated to routers. It applies only to traffic through WebAccess/VPN.

- Based on the direction of the traffic, the device Firewall rules are divided into 2 categories:
  - **Incoming** – applied to packets with a destination in the router or one of his LANs.
  - **Outgoing** – applied to packets from the router or one of his LANs.
- Each direction has its own default policy, which can be **Allow** or **Deny**.
- When a default policy is changed, the rules associated with the old policy are deactivated, and the rules configured for the new policy are activated.
- Filters are not applied to already established connections.
  - Example: If you are running a ping between two devices and add a rule denying ICMP on one or both of them, the ping will still be running since there was already an established connection before adding the rule. If you stop the ping and rerun it, the rule will apply, and the ping will not work.

**Example** of a Firewall rule: Default Incoming policy is Allow. Denied incoming traffic from IP addresses 10.40.20.1, 10.40.20.2, and 10.40.20.3 to destination network 192.168.1.0/24 on TCP ports from 50000 to 60000:

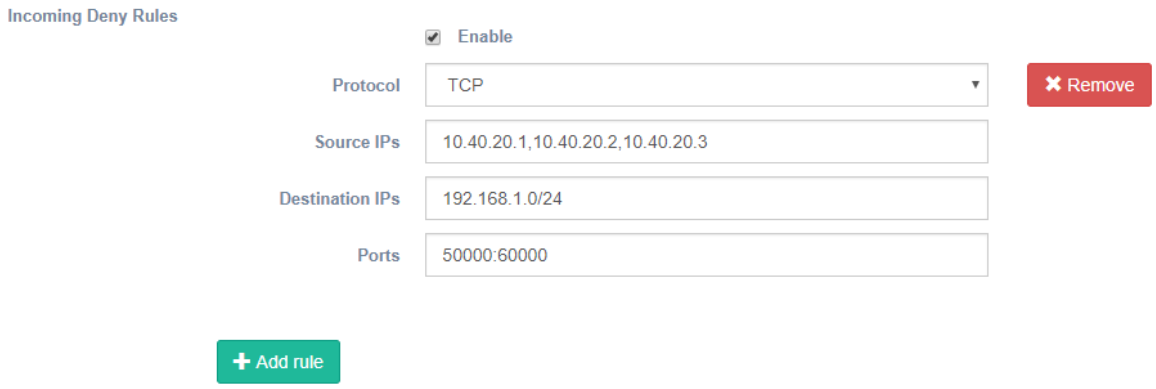



Figure 25: Device Firewall rule example

### 4.3.4 Routers: Link

Clicking on the *Link* in the Actions column in the table of Routers, a new tab/window will open with a direct login to the Router. This is via HTTPS, and WebAccess/VPN serves as a proxy, as you can see in Figure:

| Field | Options, Syntax |
|---|---|
| Protocol | TCP, UDP, or ICMP can be selected. |
| Source IPs, Destination IPs | Can be either a standalone IP, or list of IPs separated by a comma, or IP/Mask format (CIDR, e.g. 192.168.1.0/24), or a range of IP addresses in format 192.168.1.1-192.168.1.50. |
| Ports | Can be either a standalone port, or list of ports separated by a comma, or a range of ports given by a colon (e.g. 120:130). |

Table 3: Device Firewall rule – options and syntax

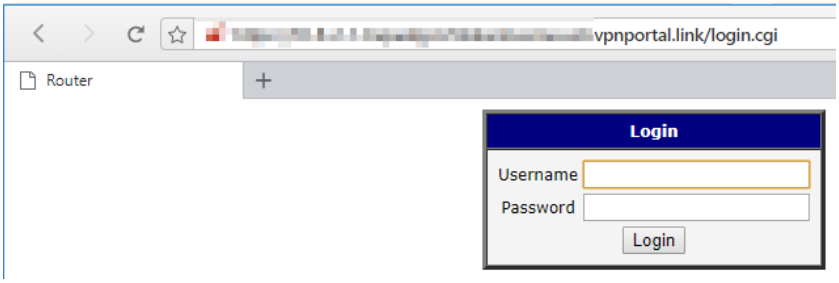



Figure 26: Routers – Link: login to Router via WebAccess/VPN as proxy

The following preconditions must be met for the *Link* to work correctly:

- The DNS records of WebAccess/VPN domain name have to be set; see Chap. 2.2.
- There has to be HTTPS service enabled in the router (*Configuration – Services – HTTP*).
- Proxy has to be enabled for the Router (Router Edit, tab Proxy).

### 4.3.5 Routers: Delete

Clicking on the *Delete* link in the table of Routers will remove the Router from WebAccess/VPN after the confirmation dialogue. As a result, the Router will lose access to the WebAccess/VPN network. The validation process has to be repeated to add the device in the future.

## 4.4 Networks

The Routers and Standalone VPN Clients added to WebAccess/VPN can see each other only after they are added to the same Network. Networks can be created or deleted on the *Networks* page; see the Figure below.

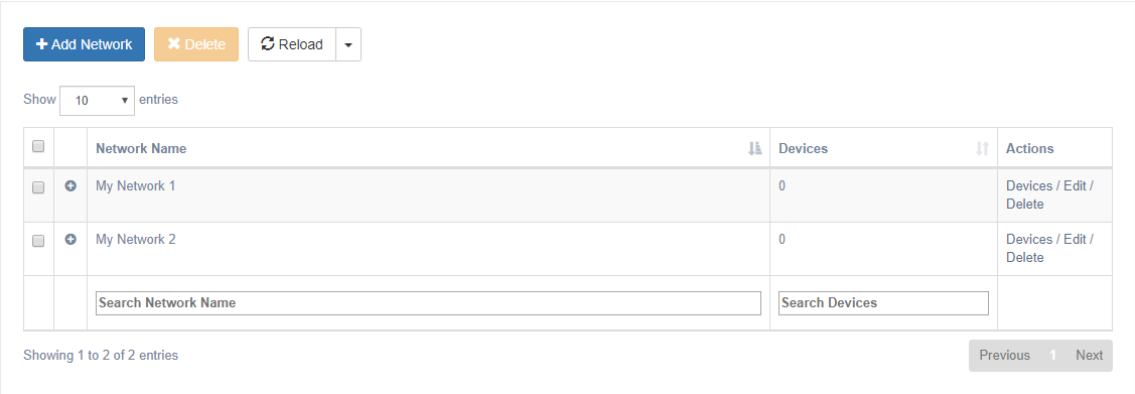



Figure 27: Networks in WebAccess/VPN

Use the blue button *Add Network* at the top of the networks list to add a new network. After the Network is created, you can add applicable firewall rules (*Edit*). The *Delete* button at the top is for network bulk deleting. Finally, the *Reload* works the same way as on the *Routers* page. To see an overview of a network, click the plus sign icon next to the network name, as shown in the Figure below:

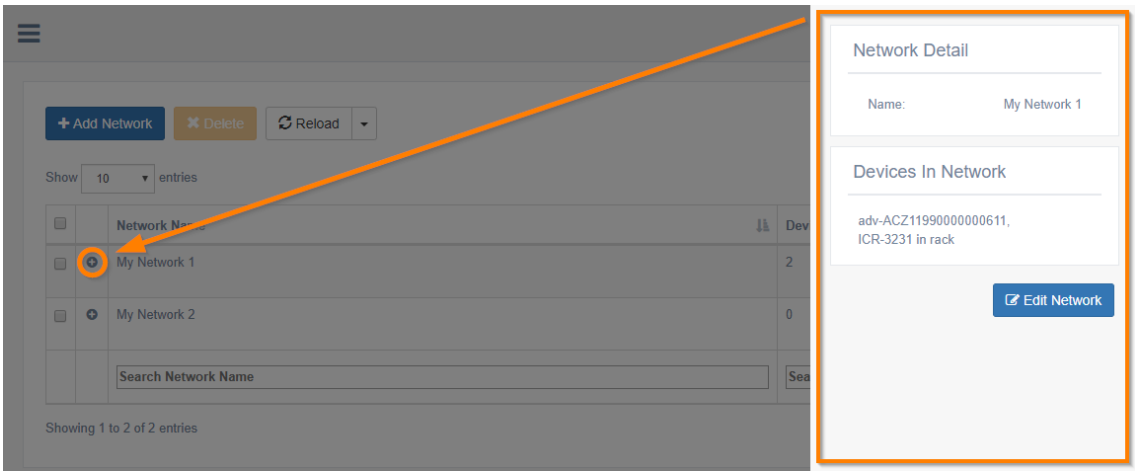



Figure 28: Networks – Network overview

The number of devices in the network is shown in the *Devices* column, and the following *Actions* are available in the next column:

- *Detail* – shows the network's main page, from where you can add/remove its devices. The exact page is displayed if you navigate to *Devices in Networks* and choose the network from the list, see section 4.5.
- *Edit* – displays a page where you can set up firewall rules or change the network's name, see 4.4.1 below.
- *Delete* – removes the network after a confirmation dialogue.

### 4.4.1 Edit – Firewall Rules for Network

When *Edit* is clicked for the network, custom firewall rules can be created for the network. For example, use the green *Add rule* button to create a filtering rule.

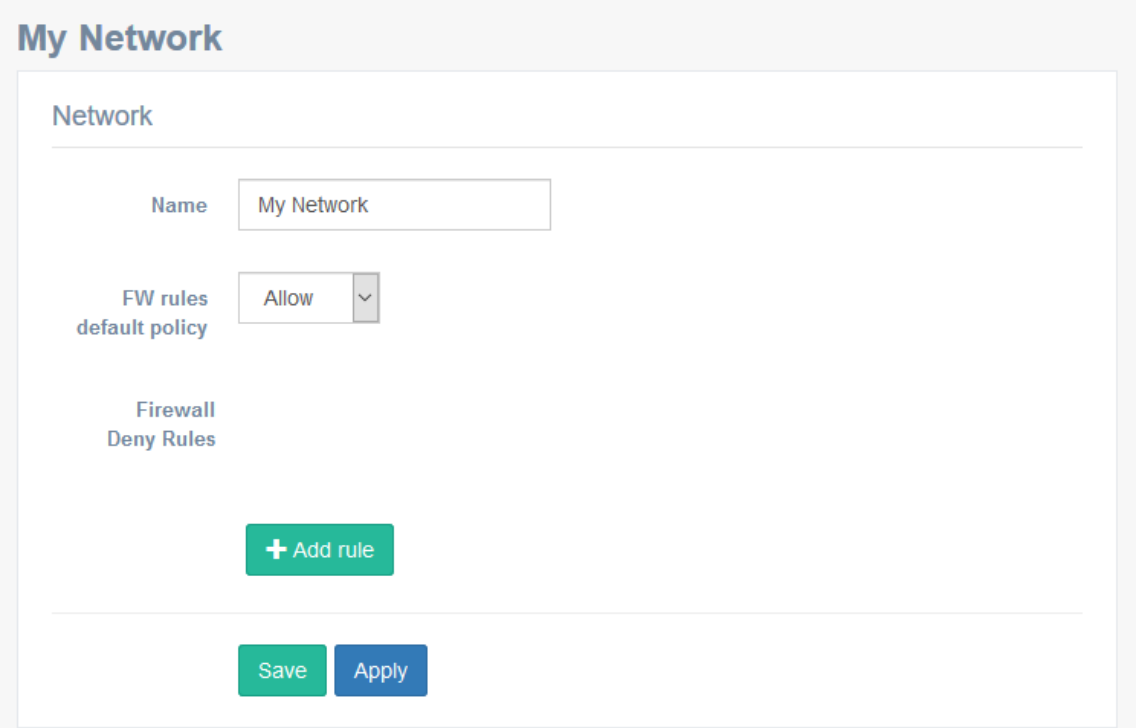



Figure 29: Networks – Firewall Rules

- Network firewall rules are only applied to traffic where both the source and the destination IP addresses belong to the same network.
- Each network has its default policy and firewall rules.
- The default policy defines what action will be taken if no rule is applied: **Allow**, or **Deny**.

- There are always 2 sets of rules for each network. The Deny set is active when the default policy of the network is set to Allow. The Allow set of rules is active when the default policy is set to Deny. They can never be both active at the same time.

**Example** of a Network Firewall rule: Default policy is Allow. This rule denies any UDP traffic in this network (ports 1 to 65535).

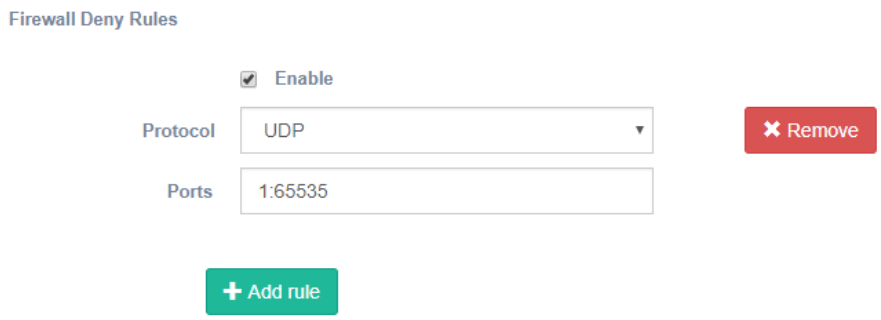



Figure 30: Device Firewall rule example

| Field | Options, Syntax |
|---|---|
| Protocol | TCP, UDP, or ICMP can be selected. |
| Ports | Can be a standalone port, a list of ports separated by a comma, or a range of ports given by a colon (e.g. 120:130). |

Table 4: Network firewall rule – options and syntax

## 4.5 Devices in Networks

Add Routers and Standalone VPN Clients to a Network or remove the devices from a Network on *Devices in Networks* page. Next, choose the network you want to edit from the dropdown menu on the left.

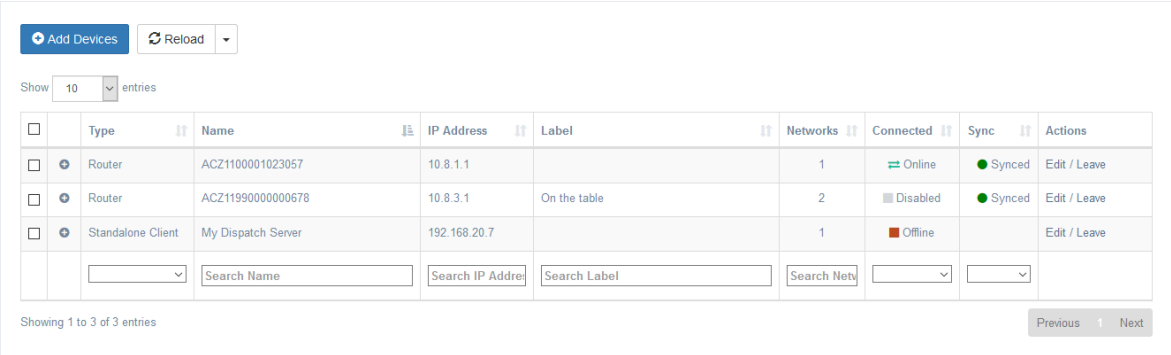



Figure 31: Devices in Networks

To add a device to a network, click the blue *Add Devices* button at the top. A pop-up dialogue will appear where you can choose the devices and confirm *Add to network*. You can choose from both Standalone VPN Clients and Routers.

Figure 32: Devices in Networks – add the device to network

The columns in the list of Devices in Network are nearly the same as on *Devices* page (there is an additional Type column and the Sync column is empty for Standalone VPN Clients). You can view details of a device by clicking on the plus icon next to the *Device Name* as in Figure 13. The *Edit* link in the *Actions* column leads to the same page where you can edit the device. Use the *Leave* link to remove a device from the network. A confirmation dialogue will appear.

## 4.6 Firewall Rules

On the *Firewal Rules* page there is an overview of all applicable firewall rules created for devices (both Routers and Standalone VPN Clients) and networks (section 4.4.1), including their status (enabled/disabled). There are 2 separate types of firewalls – Device Firewall and Network Firewall.

**Note**: Device Firewall and Network Firewall rules may be applied to each packet. When 2 devices share more than one network and start communicating, Firewall rules from multiple networks will be used.

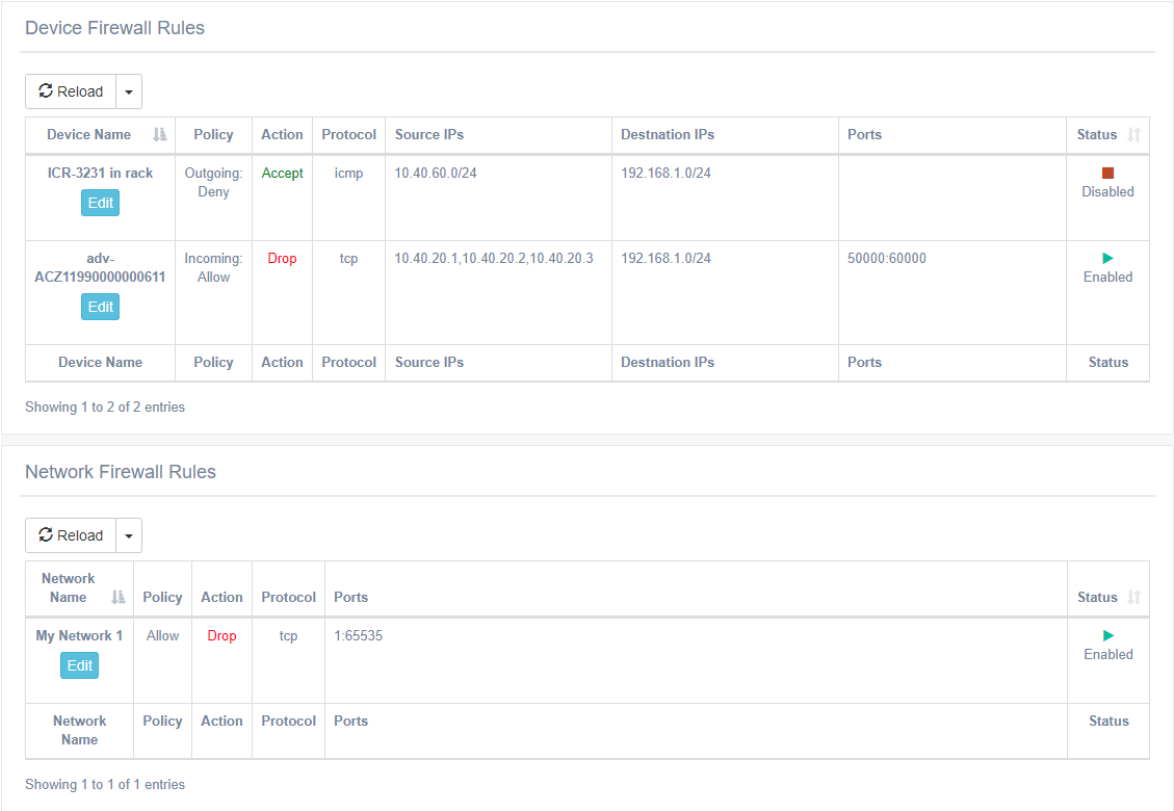



Figure 33: Firewall Rules

You can see all the rule details in the table columns. Using the *Edit* blue button, you can go directly to the Device/Network Edit page, where the Firewall rule can be changed.

If you do not see your created rule in the overview, check if the policy goes against the rule. Rules that are not applicable will not be shown on this overview page.

## 4.7 Standalone VPN Clients

The *Standalone VPN Clients* service is based on OpenVPN technology, too. Therefore, clients connected as Standalone VPN Clients can be added to Networks the same way as Routers.

> Newly added Standalone VPN Client does not automatically see any other Routers or Standalone VPN Clients. The Standalone VPN Client has to be added to a Network to see other devices in the Network (with network firewall rules applied). Firewall rules can be set for the Standalone VPN Client similarly to the Router.

Prerequisites to use a Standalone VPN Client:

- The *VPN Client Service* on the Customer Server must be running (Online) – see Chapter 4.8.1.
- A new Standalone VPN Client has to be created via the WebAccess/VPN Web UI (CS).
- The OpenVPN configuration for this client can be downloaded via a link in the Web UI and then used to initiate an OpenVPN connection between the client and the Customer Server.

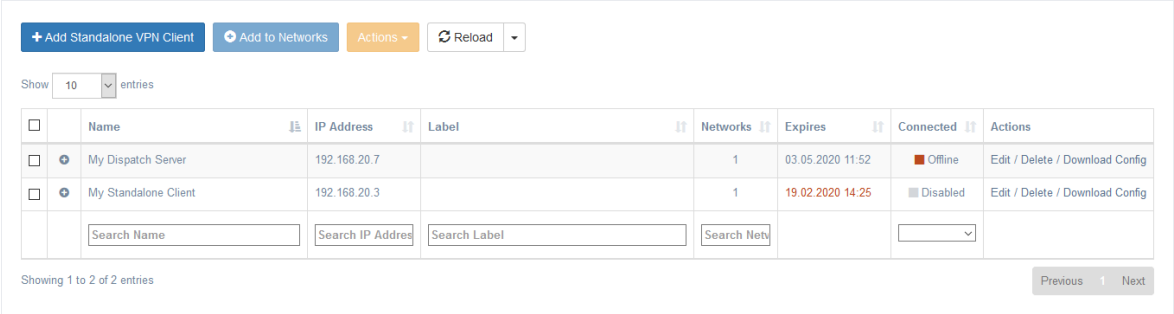



Figure 34: Manage Standalone VPN Clients

Choose the *Standalone VPN Clients* menu item to manage Standalone VPN Clients in WebAccess/VPN. A list of Standalone VPN Clients will show up as in Figure 34. Expired clients have a red-colored date on the table. It is possible to add new Standalone VPN Clients, delete them, edit some properties, or download the OpenVPN configuration file.

**To create a Standalone VPN Client:** Click on blue *Add Standalone VPN Client* button. Fill in the information as in Figure 35. You can set up the expiration of access (in days). The information provided can not be changed later (except for the Name) and will be used to create the certificate, private key, and configuration file for this Standalone VPN Client.

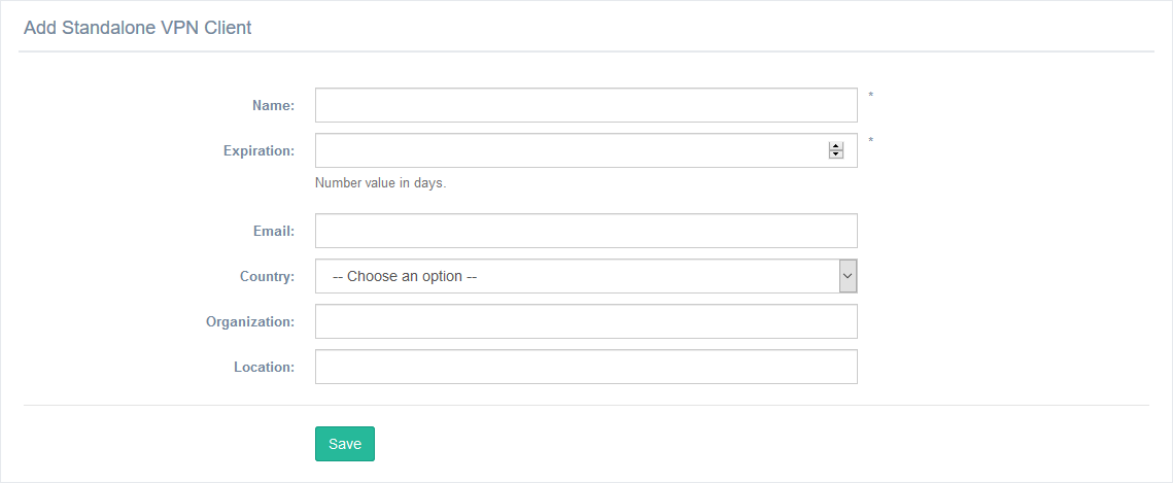



Figure 35: Add a Standalone VPN Client dialogue

**To connect as a Standalone VPN Client:** Download the client configuration file. A common OpenVPN configuration file (*.ovpn extension) contains all keys and certificates needed for an OpenVPN connection. The client configuration files can be downloaded from a list of Standalone VPN Clients in the *Actions* column through the *Download Config File* link.

**To delete a Standalone VPN Client:** Click on *Delete* in the Standalone VPN Clients table or when editing the Standalone VPN Client on tab General. This can be done in bulk in the table using checkboxes and *Actions* dropdown button. A confirmation dialogue will appear. The Standalone VPN Client will be removed, and its certificate will be revocated. This means that a Standalone VPN Client using revocated certificate will not be able to connect to WebAccess/VPN anymore. **Note:** You can temporarily disable access by disabling VPN Access the same way as you would do with the Router.

### 4.7.1 Standalone VPN Clients: Edit

It is possible to edit the Standalone VPN Client as a device similar to Router edit. However, the expiration date (and other non-required properties) can not be changed.

#### General Tab

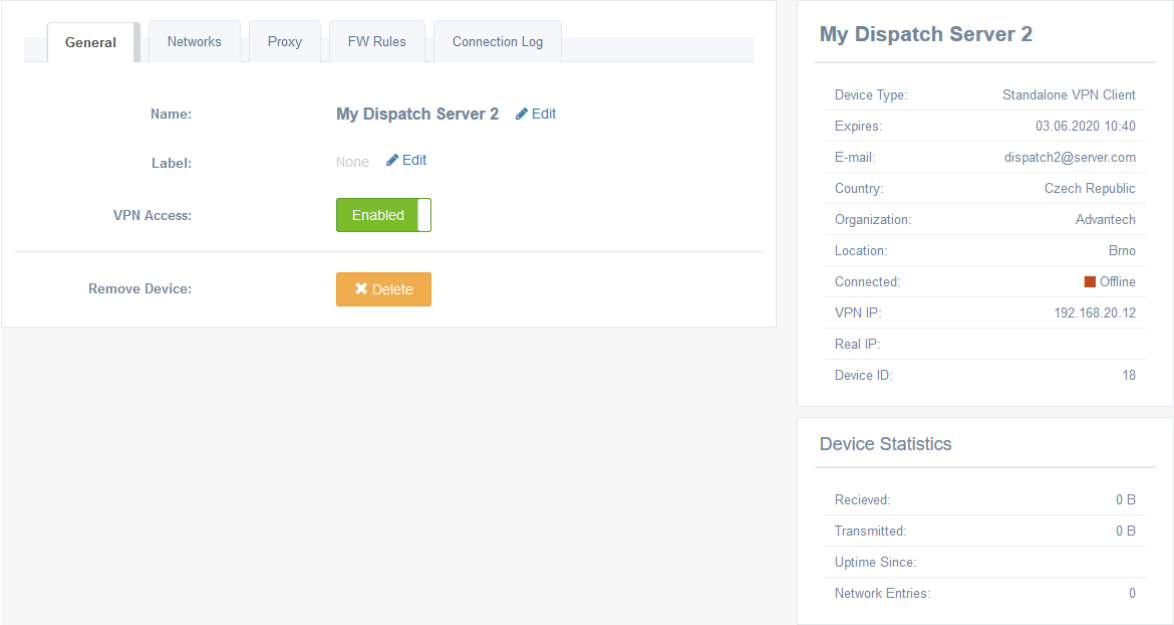



Figure 36: Edit Standalone VPN Client – General

The *General* tab is the same as for routers, except for Internet Access enable/disable. See 4.3.1. Note that the information on the right reflect device type (Standalone VPN Client) and shows expiration date and other properties.

#### Networks Tab

Add the Standalone VPN Client to a Network. Works the same way as described in 4.3.1.

#### Proxy Tab

Enable or disable the proxy for the Standalone VPN Client. Same as described in 4.3.1, except for LAN Proxy, which is unavailable. Enabling proxy here makes sense only if there is some Web interface you can go to via generated *Link to device*. This is useful e.g., for dispatch servers, intranet servers, etc. Not so for traveler's Android phones or laptops. The default state is affected by Proxy settings in *Administration – Settings*.

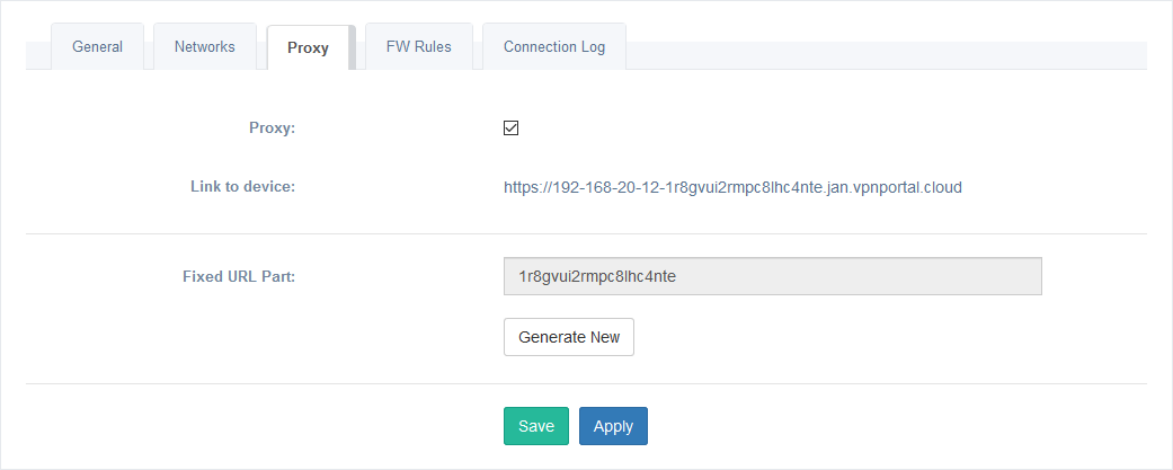



Figure 37: Edit Standalone VPN Client – Proxy

#### FW Rules Tab

Firewall rules are applicable for the Standalone VPN Client. Works the same way as described in 4.3.1 and 4.3.3, rules are visible on the *Firewall Rules* page, 4.6.

#### Connection Log Tab

Connection Log for the Standalone VPN Client. Works the same way as described in 4.3.1

### 4.7.2 Control Standalone VPN Client Service

The Standalone VPN Client service is installed and running by default. It is possible to start/stop the Standalone VPN Client service separately if you want more control. Go to *Administration – Application* as described in chapter 4.8.1 and manage the service from there.

## 4.8 Administration

The administration is accessible via the last menu item. Drop down the menu item to see the administration pages.

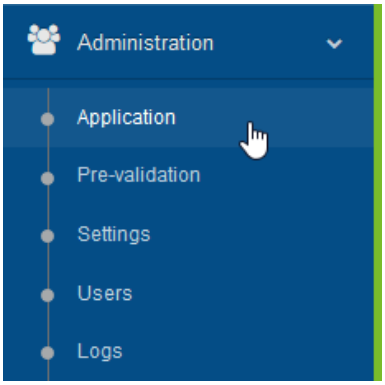



Figure 38: Administration submenu

### 4.8.1 Application

To manage the WebAccess/VPN application itself, go to the *Administration – Application* menu item. An informational screen will appear as in the Figure below. See further sections here for application information and actions that may be taken.

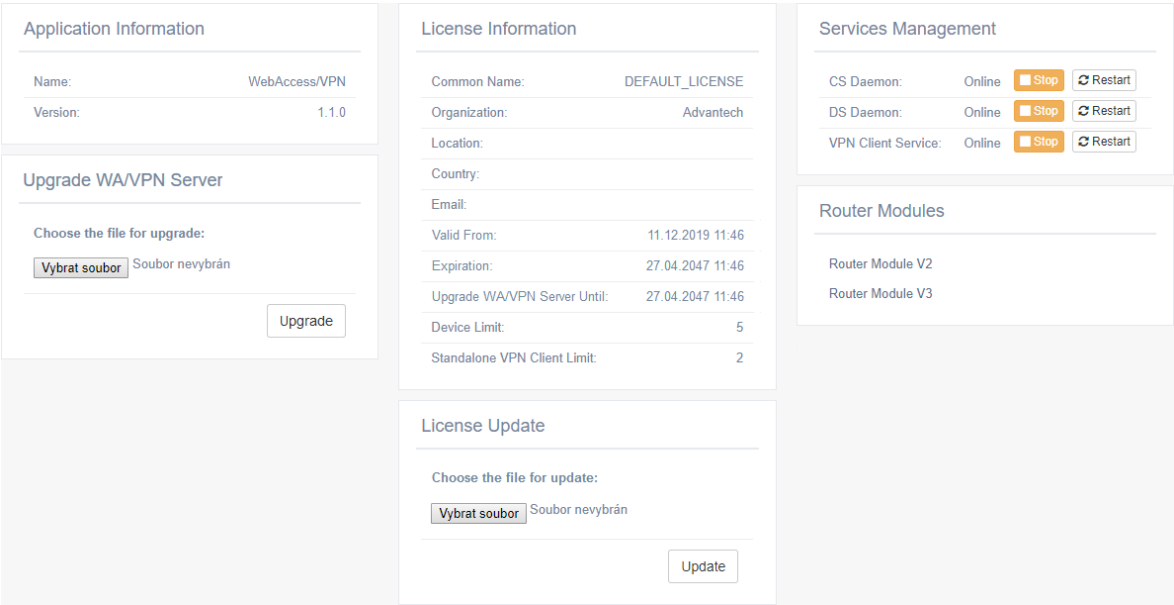



Figure 39: Application Management

### Upgrade WebAccess/VPN Server

Application information is shown in the first third, including the version. There is the possibility to upgrade WebAccess/VPN server from the tarball file. Choose the proper file and click the *Upgrade* button.

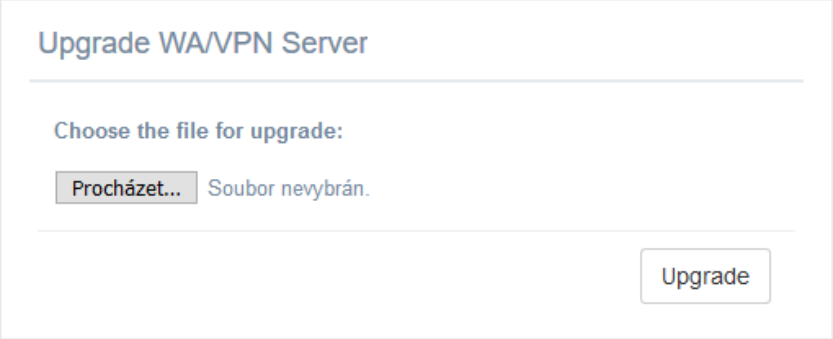



Figure 40: Upgrade WebAccess/VPN Server

Allow the WebAccess/VPN a few minutes to upgrade. Do not refresh the browser during the upgrade, as there is currently no progress bar showing the state of the upgrade.

The free demo version from Amazon Marketplace can not be upgraded or licensed to the production version. The possibility to upgrade can also be affected by the license used (see the date in *Upgrade WA/VPN Server Until* in the *License Information* box under *Administration/Application* menu item).

### Update License

There is license information in the middle, showing the limits and expiration of the license. There is the possibility of updating the license file. Choose the .license license file and click the *Update* button.

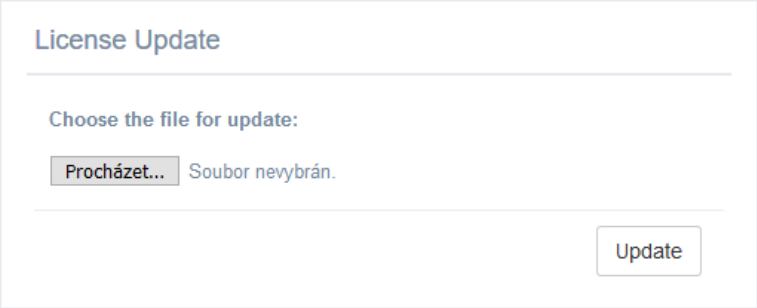



Figure 41: Update license of WebAccess/VPN Server

### Services Management

In the top-right part of the screen, you can manage the software parts (services) of WebAccess/VPN. You can stop/start or restart particular services from here. All services run on the same server. CS Daemon is WebAccess/VPN UI itself, DS Daemon tells the routers where they should connect as described in the Introduction. The VPN Client Service is for Standalone VPN Clients. Services management is helpful for troubleshooting – it is possible to check whether services are running.

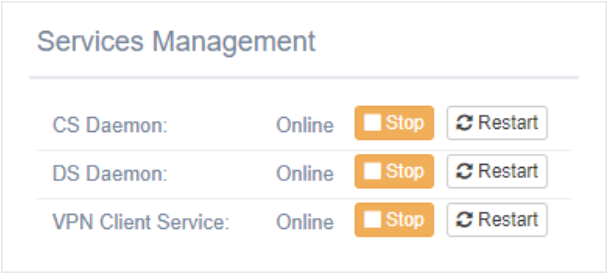



Figure 42: WebAccess/VPN services management

### Download Router Apps

You can easily download router apps for your Advantech routers to add them to WebAccess/VPN.

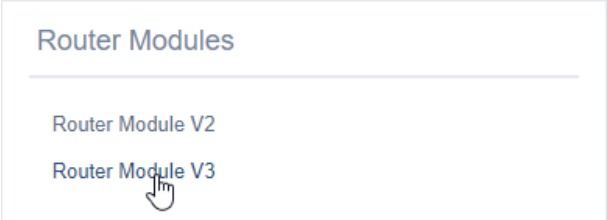



Figure 43: Download router apps for routers

### 4.8.2 Pre-validation

List of routers can be uploaded on *Administration – Pre-validation* page. These routers are then validated automatically when trying to connect to WebAccess/VPN. The VPN tunnel is established, and the routers can be found on *Routers* page. After auto validation, they are removed from the pre-validation page. Click the *Upload New List* blue button to upload the list.

> The list of pre-validated routers is always overwritten by uploading the new one.

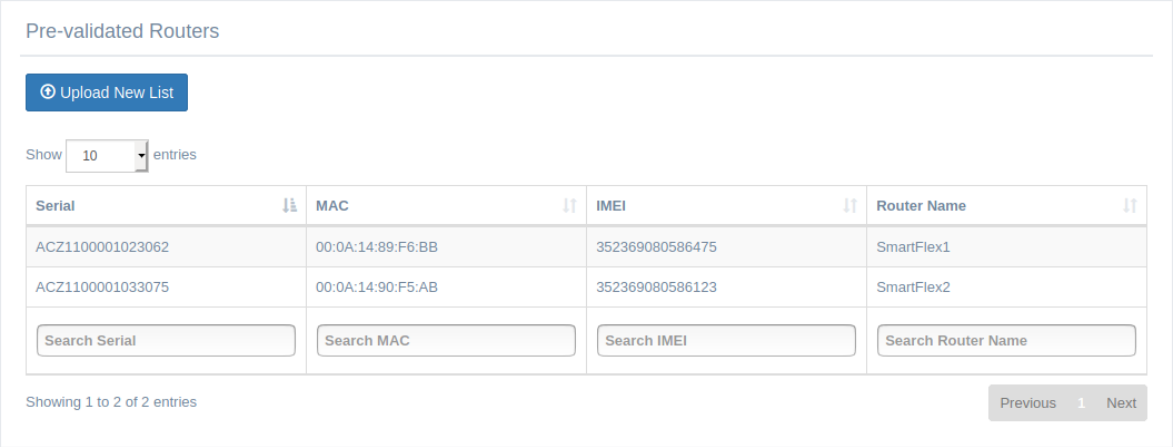



Figure 44: Logs

The format of the list file has to be a TXT file with the following structure. Note that the number of commas has to remain the same on all lines. A sharp character can be used as a comment.

```
# SERIAL,                MAC,                IMEI,          NAME
#############################################################
ACZ1100001023062, 00:0A:14:89:F6:BB, 352369080586475, SmartFlex
ACZ1100001033075, 00:0A:14:90:F5:AB, 352369080586123,
```

- serial number (mandatory)
- MAC address (mandatory)
- IMEI of the cellular module (mandatory)
- name (not mandatory)

### 4.8.3 Settings

The *Administration – Settings* page contains WebAccess/VPN parameters that can be configured. See the items explained in the table below.

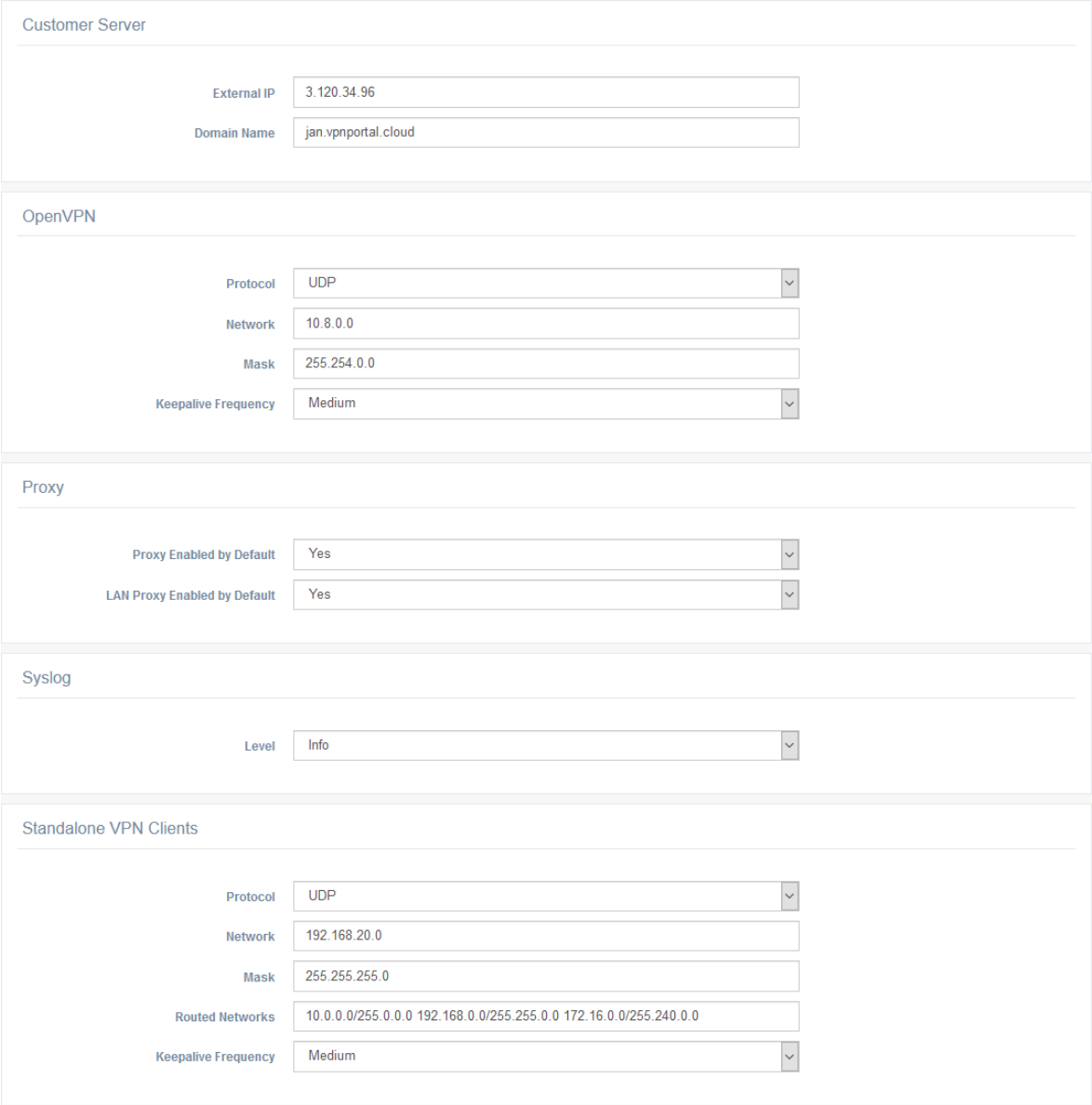



Figure 45: Settings of WebAccess/VPN

| Setting | Description |
|---|---|
| **Customer Server** | |
| External IP | The IP address of CS will be given to routers. It has to be reachable from routers. Useful when moving your WebAccess/VPN to another IP. |
| Domain Name | The domain name of CS. Useful when moving your WebAccess/VPN to another domain name. |
| **Syslog** | |
| Level | Verbosity level of the Syslog. |
| **Proxy** | |
| Proxy Enabled by Default | The default state of Proxy for the newly added device. It can be managed additionally in device Edit. |
| LAN Proxy Enabled by Default | The default state of LAN Proxy for newly added Router. It can be managed additionally in Router Edit. |
| **OpenVPN** | |
| Protocol | Based on this setting, the OpenVPN Tunnel with Routers is established via UDP (default) or TCP. Useful for cases when the firewall blocks UDP. **Note:** when running WebAccess/VPN on Amazon according to installation described in 2.2, do not forget to check and update your Security Group firewall rules accordingly. |
| Network Mask | The pool of virtual addresses for routers (and possibly for devices behind them). Make sure this pool is large enough to cover all your routers (The system reserves 255 addresses for each router). It can only be changed while there are no validated routers in the system. |
| Keepalive Frequency | This represents the interval between pings used to check individual devices' connection state. The device is marked as Offline after 2 consequent ping checks fail (while no other traffic passes through the tunnel). Lower ping frequency means lower data consumption but higher delays in updating the connection state.<br><br>**Very low**: ping once every 300 s<br>**Low**: ping once every 117 s<br>**Medium**: ping once every 40 s (default)<br>**High**: ping once every 15 s |

Continued on next page

Continued from previous page

| Device Property | Description |
|---|---|
| **Standalone VPN Clients** | |
| Protocol | Based on this setting, the OpenVPN Tunnel with Standalone VPN Clients is established via UDP (default) or TCP. **Note:** when running WebAccess/VPN on Amazon according to installation described in 2.2, do not forget to check and update your Security Group firewall rules accordingly. |
| Network Mask | The pool of virtual addresses that will be assigned to Standalone VPN Clients. **Note:** Both OpenVPN networks (VPN clients, Routers) will be restarted automatically. |
| Routed Networks | IP ranges that will be routed to the tunnel. By default, all private IP ranges are listed. |
| Keepalive Frequency | This represents the interval between pings used to check individual devices' connection state. The device is marked as Offline after 2 consequent ping checks fail (while no other traffic passes through the tunnel). Lower ping frequency means lower data consumption but higher delays in updating the connection state.<br><br>**Very low**: ping once every 300 s<br>**Low**: ping once every 117 s<br>**Medium**: ping once every 40 s (default)<br>**High**: ping once every 15 s |

Table 5: WebAccess/VPN Settings items

### 4.8.4 Users

To manage users and their roles, go to the *Administration – Users* menu item. You can see all configured users in a table on the *Users* page. It is possible to edit, remove, or add new user accounts.

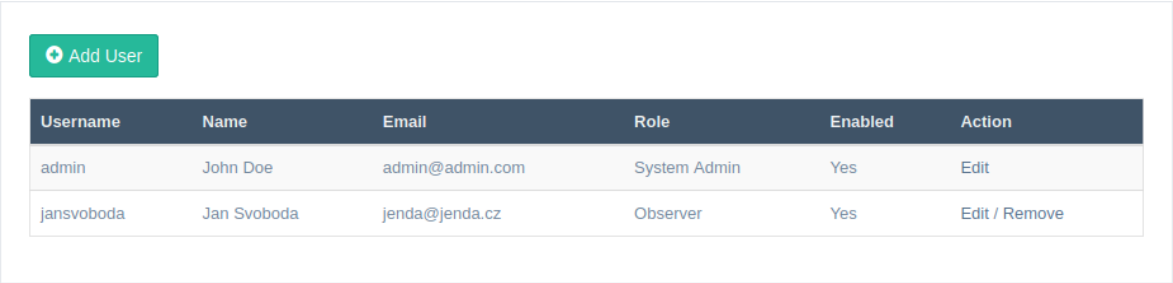



Figure 46: Users management

Click the *Add User* button to add a new user. A dialogue appears (see the next Figure) where it is possible to enter new user account information. The same dialogue is used for editing the information of an existing user.

You can enter the basic identification information (Username, Name, Email, Password), specify the user role (see the list below) and enable/disable the account. If disabled, the account does not allow login, but the information about the user is stored in WebAccess/VPN and the account can be enabled again in the future (by the user with the System Admin role).

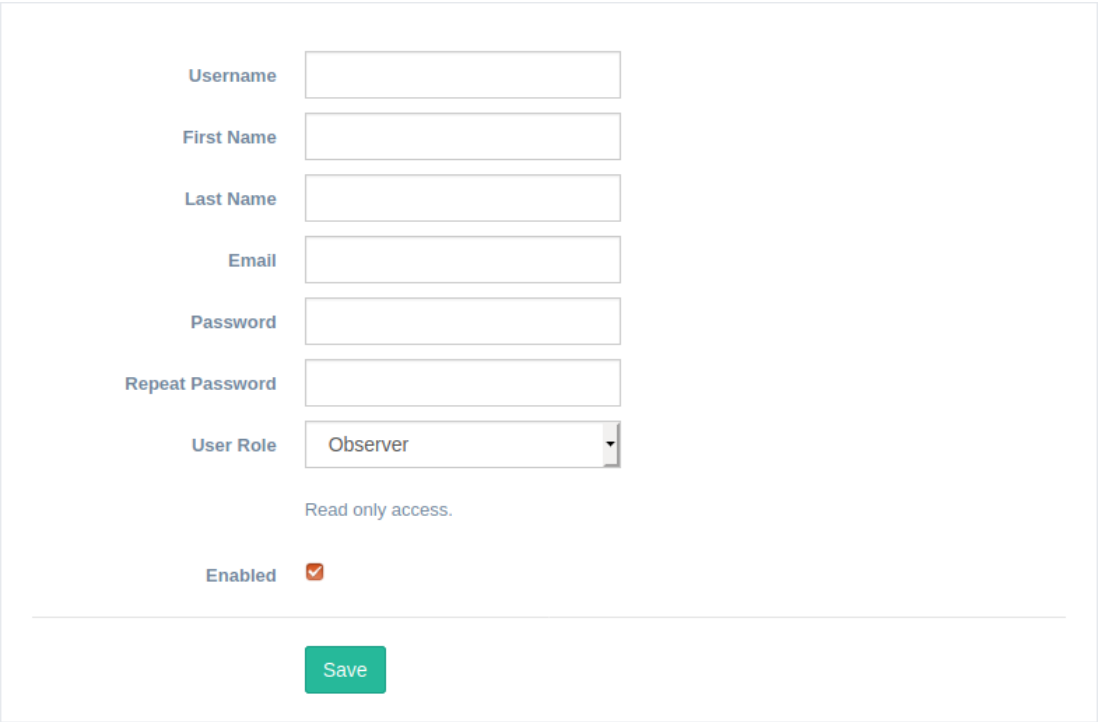



Figure 47: User Edit

Roles are defined as follows. The definition is hierarchical – it means that a higher role contains rights of the predecessor role:

- **Observer** – read-only access. This is the default role.
- **Device Admin** – for device administration (can validate and edit devices – Routers and Standalone VPN Clients).
- **Network Manager** – for network management (can add/remove the device to/from the network, can add and edit firewall rules for networks).
- **Network Admin** – for networks administration (can create, edit and delete networks).
- **System Admin** – full access for user management (can add, edit or delete users), change settings and administer the application.

### 4.8.5 Logs

To access Logs, go to the *Administration – Logs* menu item. The page with Logs will appear as in the Figure below.

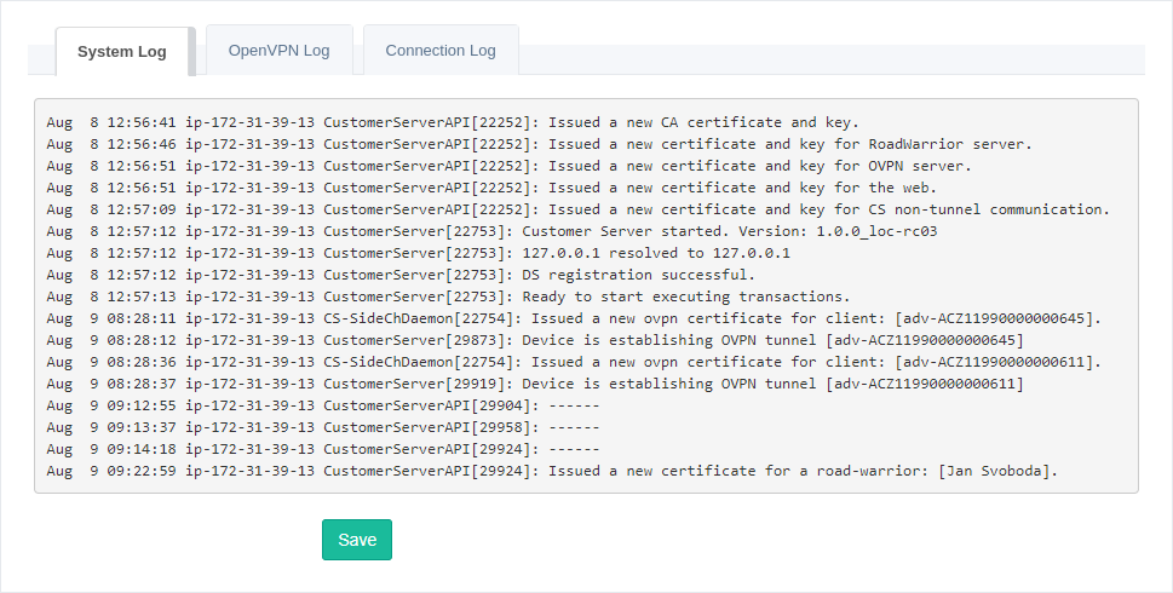



Figure 48: Logs

It is possible to switch between the *SystemLog*, *OpenVPN Log* and *Connection Log* view (Connection Log contains information of all devices connecting to WebAccess/VPN on one place). All logs can be downloaded in a single TXT file by clicking on the Save button under the logs. There will be sections with all three types of logs in the downloaded file. This file can be shared with technical support in case of difficulties.

# 5. Advanced Management

## 5.1 Password Reset

The password reset can be achieved only via SSH login to the system, where WebAccess/VPN is running. Login via SSH, go to /opt/vpnportal, and run the password reset script according to the following commands:

```
cd /opt/vpnportal
./reset_admin_passwd.sh
```

As a response, the newly generated password will be printed on the console. Copy or write down this new password. You can change it later in *Administration – Users*.

```
vpn@vpn:/opt/vpnportal$ ./reset_admin_passwd.sh
New password for admin is: "w1hH4LovOnvB".
vpn@vpn:/opt/vpnportal$
```

# 6. Troubleshooting

## 6.1 How to check WebAccess/VPN Running Services

On the *Administration – Application* page of the WebAccess/VPN UI, the running services may be checked, stopped, started, or restarted. See Chapter 4.8.1 for details.

## 6.2 How to Access Logs

### Router Logs

On routers, the log messages can be seen on the router app's *VPN Portal* web page:
*OpenVPN Tunnel* – shows the status of the OpenVPN tunnel.
*WebAccess/VPN* – shows the status of the router app.

### WebAccess/VPN Logs

On the *Administration – Logs* page of the WebAccess/VPN UI, the System Log, the OpenVPN Log, and the Connection Log can be viewed. See Chapter 4.8.5 for details.

# 7. Related Documents


**[1]** Advantech Czech: **v2 Configuration Manual** (MAN-0021-EN)
**[2]** Advantech Czech: **SmartStart Configuration Manual** (MAN-0022-EN)
**[3]** Advantech Czech: **SmartFlex Configuration Manual** (MAN-0023-EN)
**[4]** Advantech Czech: **SmartMotion Configuration Manual** (MAN-0024-EN)
**[5]** Engineering Portal: **icr.advantech.com**

# A. Standalone Hardware Test

**Test Description:** A single Network was created in WebAccess/VPN. All the devices were added to this Network. Then, random pairs of devices were made to communicate with each other. Next, the device from each pair was randomly selected to be the active ping sender (the other device only listened and replied to pings). Traffic was regulated by ping interval and payload size.

**Hardware used for the test:** WebAccess/VPN was running on a PC with the following processor: Intel(R) Xeon(R) E3-1245 v5 @ 3.50GHz (4 cores).

**Measurement:** The load of the CPU was measured with the "top" program.
The traffic amount was measured with the "nload" program.

**Test Results:** See the table below:

| Number of devices → Traffic per device ↓ | 10 | 100 | 1000 |
|---|---|---|---|
| 0 | 0.04, 0.03 | 0.00, 0.02 | 0.01, 0.05 |
| 0.2 kbps | 0.01, 0.02 | 0.05, 0.07 | 0.12, 0.11 |
| 2 kbps | 0.04, 0.04 | 0.02, 0.05 | 0.14, 0.17 |
| 20 kbps | 0.06, 0.03 | 0.11, 0.15 | 0.31, 0.41 |
| 200 kbps | 0.07, 0.12 | 0.44, 0.47 | 1.09, 1.04 |
| 2 Mbps | 0.40, 0.45 | 0.98, 0.99 | |

Table 6: Performance test results

Overall tunnel traffic for any combination is the product of the number of devices and traffic per device, e.g. for 1000 devices and 20 kbps traffic, the overall tunnel traffic was 20 kbps x 1000 = 20 Mbps.

| Legend |
|---|
| Green colored cells – traffic and number of devices were managed. |
| Red colored cell – overall traffic was too high and could not be managed. |
| Two number values in the cells represent the CPU load average for 1 and 5 minutes of run. These are taken from the "top" program. |

**Findings and Recommendations:** See section 2.6.2.