# WebAccess/VPN

## APPLICATION NOTE

Manage VPN

List of Devices

Show 10 entries  Search:

| ☐ | | Device Name | IP Address | Name | Networks | Connected | Synced | Actions |
|---|---|---|---|---|---|---|---|---|
| ☐ | ⊕ | adv-00.0A.14.DE.F0.A1 | 10.8.1.1 | adv-00.0A.14.DE.F0.A1 | 0 | 🟥 Offline | ● | Edit / Manage / Delete |
| ☐ | ⊕ | adv-5516738 | 10.8.4.1 | adv-5516738 | | ⇄ Online | ● | Edit / Manage / Delete |
| ☐ | ⊕ | adv-B0.D5.CC.EA.26.86 | 10.8.2.1 | adv-B0.D5.CC.EA.26.86 | | 🟥 Offline | ● | Edit / Manage / Delete |
| ☐ | ⊕ | adv-IAD1004822 | 10.8.3.1 | adv-IAD1004822 | | 🟥 Offline | ● | Edit / Manage / Delete |
| | | Search Device Name | Search IP Address | Search Name | | | | |

Showing 1 to 4 of 4 entries  Previous 1 Next

ADVANTECH

# Used Symbols

*Danger* – Information regarding user safety.

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

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

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

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

techSupport@advantech-bb.com

Please see http://ep.advantech-bb.cz/devzone for more information.

# Software Version

This Application Note describes the *WebAccess/VPN* in version **1.1.1**.

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic.
Document No. APP-0021-EN, revision from November 18, 2020. Released in the Czech Republic.

# Contents

# List of Figures

# List of Tables

# 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.

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 – just upload the user module. OpenVPN settings are then pushed to 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 User module *VPN Portal* has to be uploaded to the router. The routers are then connecting to these two entities:
- **Dispatch Server (DS)** – a registration service that 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) are 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 you can see 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) which is an OpenVPN server with Web UI, and this controls traffic. The CS lists the Router as a new router waiting for validation.

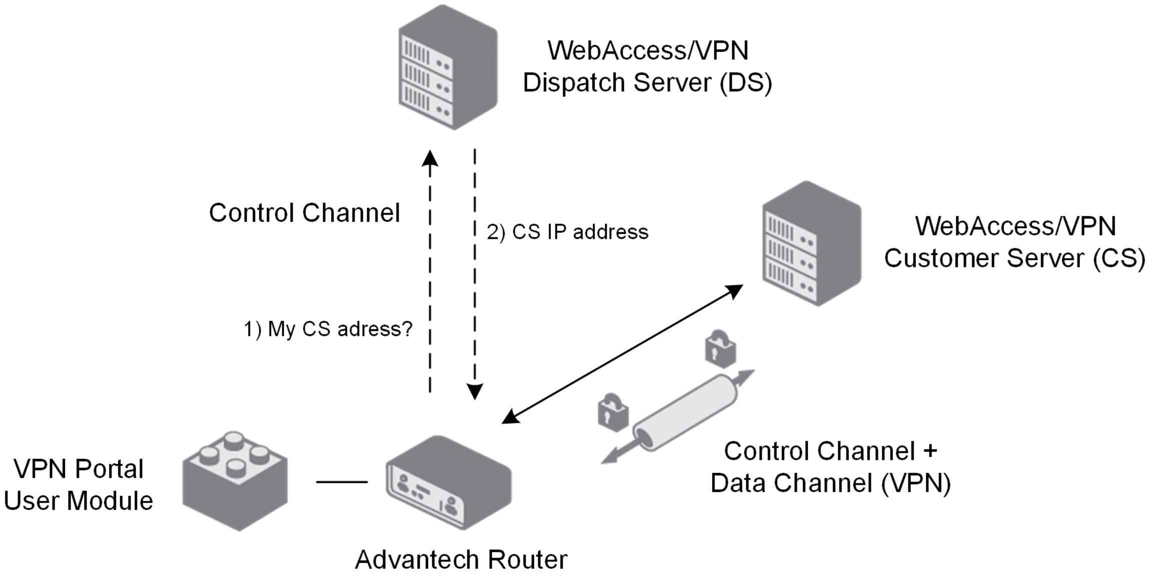


Figure 1: The basic parts of the WebAccess/VPN system, showing a new router connection

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.

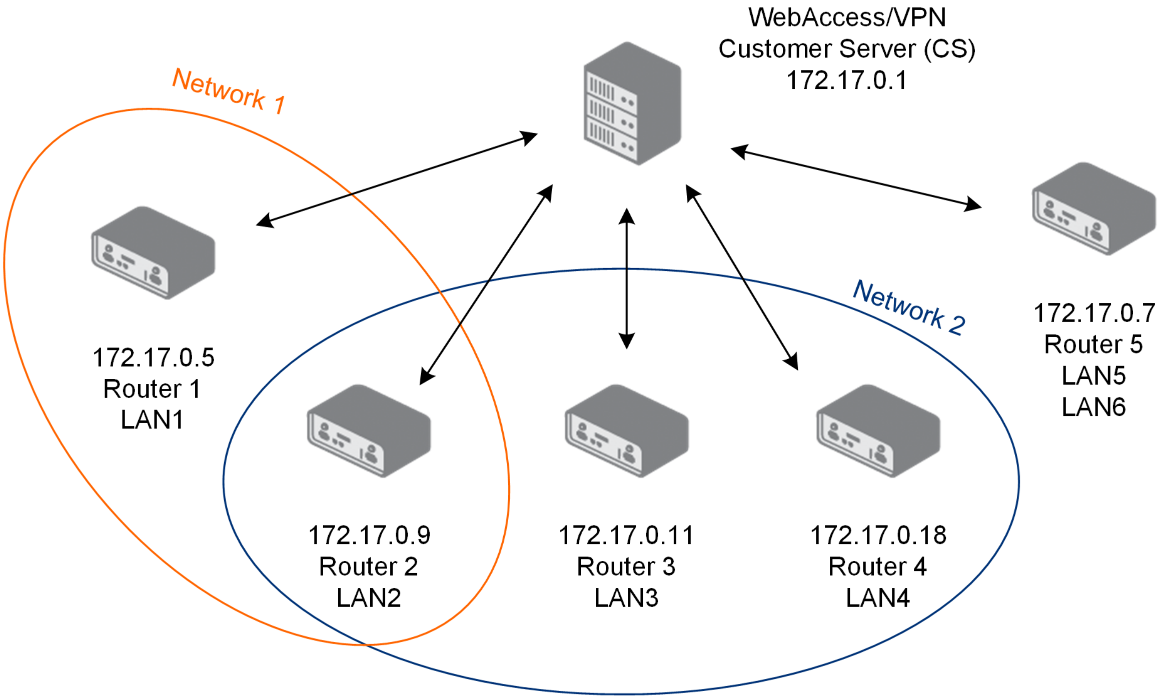


Figure 2: Networks – groups of routers

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 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

## 2.1 Free Demo Installation on Amazon Marketplace

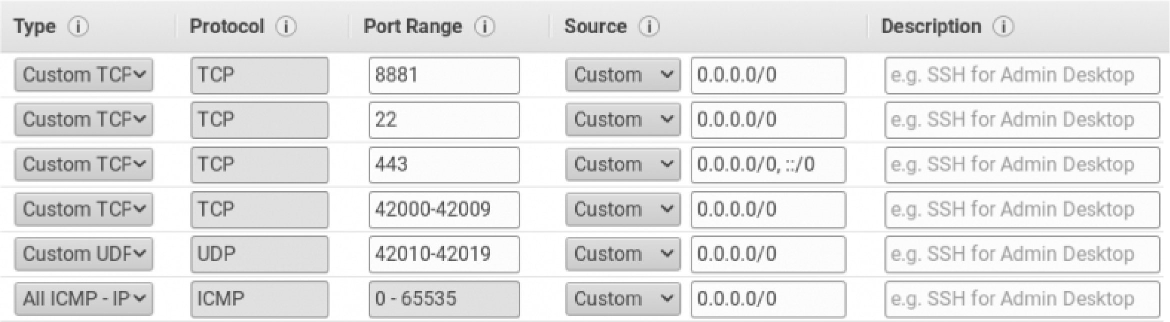
⚠ The free demo version from Amazon Marketplace has a limitation of 5 routers and 2 standalone VPN clients. This version is not intended for production usage and can not be upgraded or licensed to the production version.

The free version of the product is available on the Amazon Marketplace. Following instructions will guide you through the process of running the product step by step:

1. Locating the image on Amazon Marketplace
   - Open up the Amazon Marketplace at https://aws.amazon.com/marketplace.
   - After typing in the "WebAccess/VPN" into the search box you will get the matching hit and can follow to the "WebAccess/VPN Free" product.
2. Selecting the image
   - On the "WebAccess/VPN Free" product page click on the "Continue to Subscribe" button.
   - If you are not logged in to your Amazon AWS (Amazon Web Services) in the running browser session, you will be asked to do so.
   - When starting your first image on Amazon, you will be asked to accept the AWS agreement.
   - In this agreement, the terms summarize costs above the ones Amazon is charging (we do not charge anything for the free product version).
   - There may be some delay before Amazon processes your acceptance of AWS agreement though it should not take more than a minute. Once the AWS agreement is done, you may continue by clicking on "Continue to configuration" button.
3. Configuring image startup
   - In the next step, you select the Region you want to run the image at and click on the "Continue to Launch" button.
   - Now, select the "Launch through EC2" Action and confirm it by the "Launch" button. Also, note that here you can inspect the instructions on a proper setup by clicking on the "Usage Instructions".
   - The Instance type suggested in the next step, t2.micro, is quite okay for running the free version of the product (in fact, it is enough for production use as well while the number of routers stays low). But because the routers need to be able to connect to the server, you need to configure the so-called Security Groups. Therefore, click on the "6. Configure Security Group" tab.

- At the security groups screen, you should add rules to allow several ports and port ranges. Basically, you need to open these ports:
  - Allow **TCP** ports 22, 443, 8881, 42000 – 42009.
  - Allow **UDP** ports 42010 – 42019.
  - Allow **ICMP** protocol – all traffic.

  The resulting screen may look like the one in Figure 3.



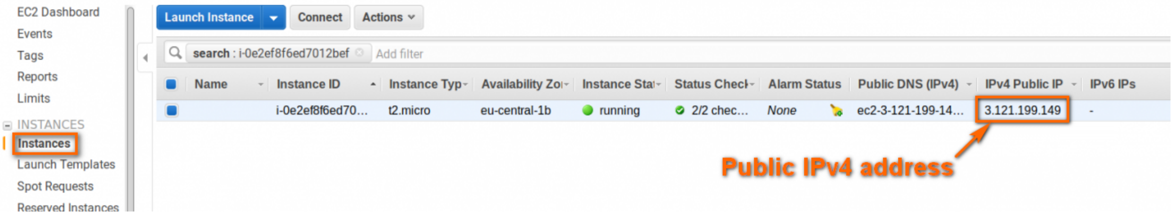
| Type ⓘ | Protocol ⓘ | Port Range ⓘ | Source ⓘ | | Description ⓘ |
|---|---|---|---|---|---|
| Custom TCP | TCP | 8881 | Custom | 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| Custom TCP | TCP | 22 | Custom | 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| Custom TCP | TCP | 443 | Custom | 0.0.0.0/0, ::/0 |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

Figure 3: Configuring security group

- Afterwards you click on "Review and Launch" followed by the "Launch" button. Note that after clicking on Launch, you may be asked to create a key pair (if you haven't done that already when running other images on Amazon EC2). Download the key pair and click on "Launch Instances" button.
- Once the instance is launched you will be redirected to "Launch Status" page. From here you could continue by clicking on the first link (the alphanumeric instance identifier) or View Instances on the bottom right.

4. Connecting to SW setup wizard

- To connect to the running server you need its IP address. That can be found in the IPv4 Public IP column in the instances list (see Figure 4).



| ■ | Name | Instance ID | Instance Typ | Availability Zo | Instance Stat | Status Check | Alarm Status | Public DNS (IPv4) | IPv4 Public IP | IPv6 IPs |
|---|---|---|---|---|---|---|---|---|---|---|
| ■ | | i-0e2ef8f6ed70... | t2.micro | eu-central-1b | ● running | ✓ 2/2 chec... | None | ec2-3-121-199-14... | 3.121.199.149 | - |

Figure 4: Get public IPv4 address

- Once you have the IP, you can connect to the running image on this address (substitute the instance-IP with your real image IP address): **https://<instance-IP>:8881**

5. Installing the server

   - You will see the installation wizard of the software that will guide you through the security setup (generating or importing certificate), network settings, domain setup, password setup and EULA acknowledgment. For more details about the wizard see 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 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 controls the certificates and keys, and Advantech has no access. The installation process is described below.

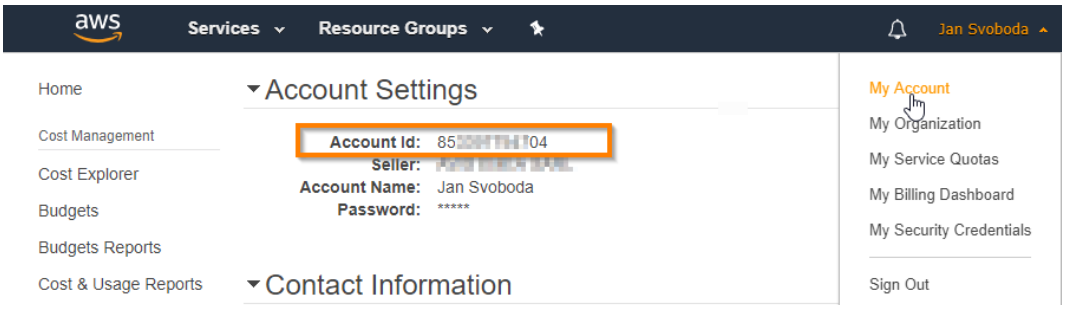
**Prerequisites for the install:**

- 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 setup 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 to Advantech using the following e-mail address: vpn.aws@advantech.com



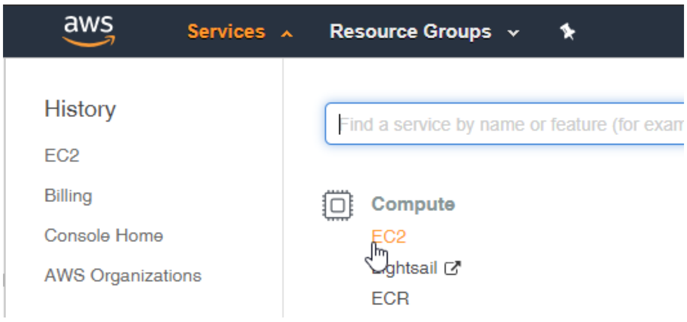
Account Settings

Account Id: 85[redacted]04
Seller: [redacted]
Account Name: Jan Svoboda
Password: *****

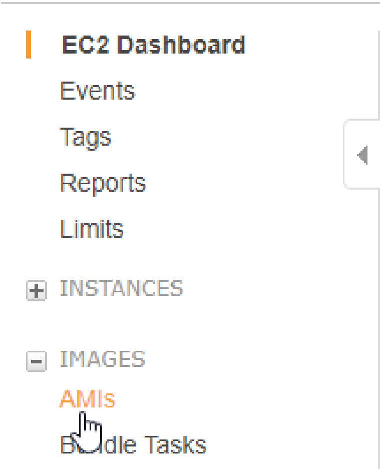
Contact Information

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

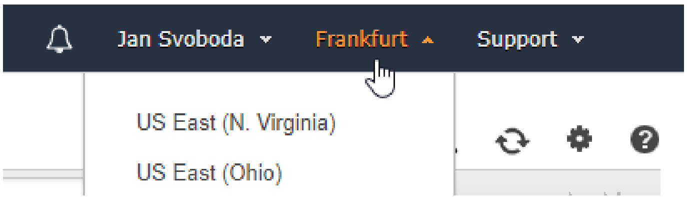
2. Now login to your Amazon AWS account and select Services, **EC2**.



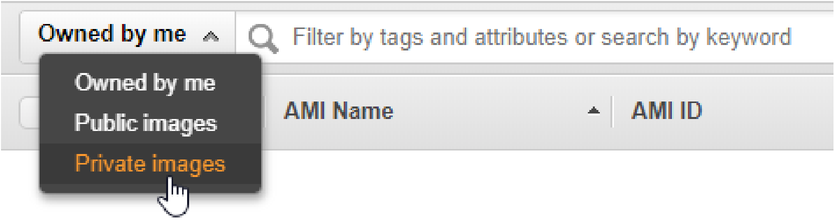
3. Select the **AMIs** form Images menu on the left.



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 e-mail address: vpn.aws@advantech.com.
   The image will then be copied to your location.

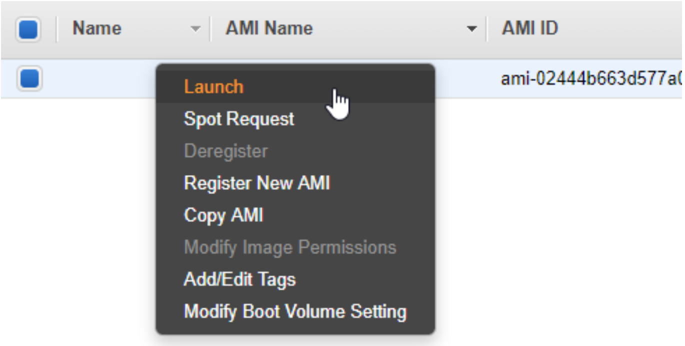


5. Change the filter of images to **Private images**.

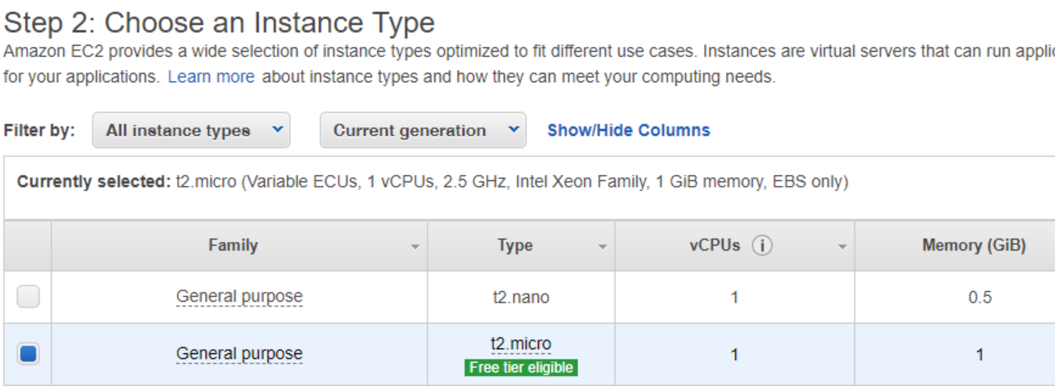


6. Now the shared image from Advantech should be visible under the name **WebAccess/VPN**. You can also check the owner of the image is 686278836833.
7. Right click on the image and select *Launch* to create the instance.

> 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.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applic
for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

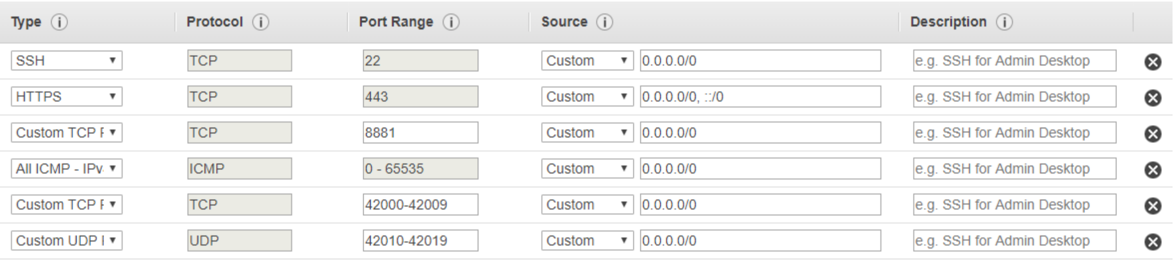
**Currently selected:** t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

| | Family | Type | vCPUs ⓘ | Memory (GiB) |
|---|---|---|---|---|
| □ | General purpose | t2.nano | 1 | 0.5 |
| ■ | General purpose | t2.micro<br>Free tier eligible | 1 | 1 |

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 system should be active, do not remove it. Add the following additional rules:

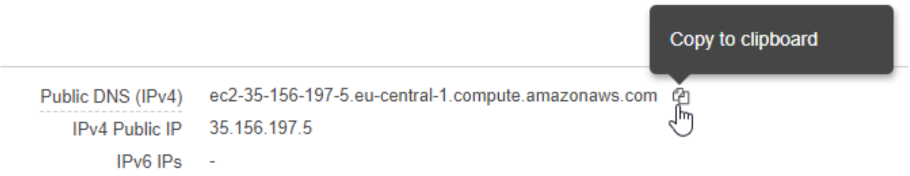
   - Allow **HTTP** traffic on port **80**.
   - Allow **HTTPS** traffic on port **443**.
   - Allow **TCP** port **8881**.
   - Allow **ICMP** protocol – all traffic.
   - Allow **TCP** ports from **42000 to 42009**.
   - Allow **UDP** ports from **42010 to 42019**.



| 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). Choose the instance and look below the table at the *Description*. Find Public DNS or IP and copy it to the clipboard.

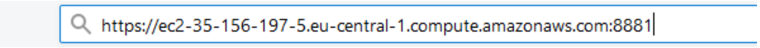


Public DNS (IPv4) ec2-35-156-197-5.eu-central-1.compute.amazonaws.com

IPv4 Public IP 35.156.197.5

IPv6 IPs -

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://ec2-35-156-197-5.eu-central-1.compute.amazonaws.com: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 wizard, go to 2.5

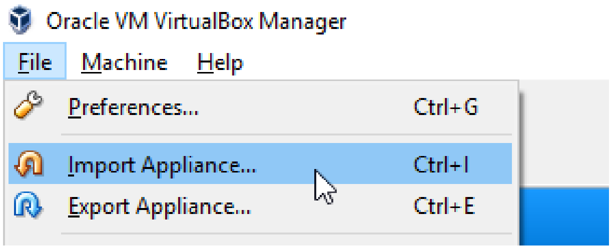
## 2.3 On-Premises Installation – VirtualBox

Both Dispatch Server and Customer Server installed on-premises as VirtualBox appliance. Provided appliance uses Ubuntu 18.04 LTS operating system and contains the installer of WebAccess/VPN. Since this is the on-premises version, sole customer is responsible for the run of the WebAccess/VPN system, its security and updates, including operating system provided in the appliance.

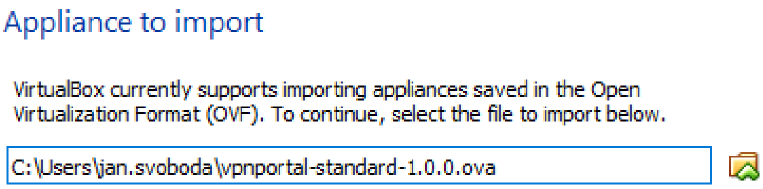
**Prerequisites:**

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



Appliance to import

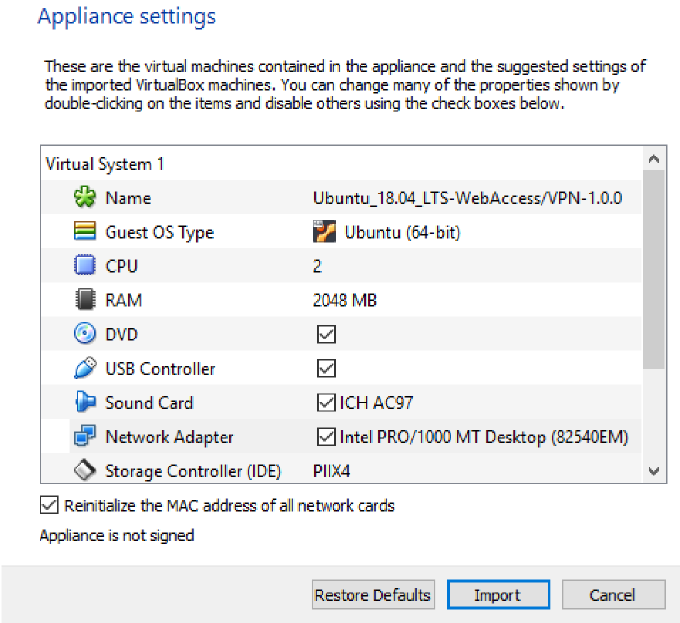
VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

C:\Users\jan.svoboda\vpnportal-standard-1.0.0.ova

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.



Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

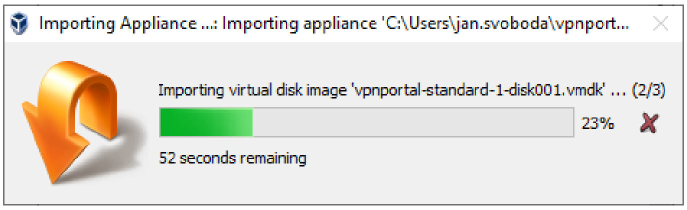
Virtual System 1

| | |
|---|---|
| Name | Ubuntu_18.04_LTS-WebAccess/VPN-1.0.0 |
| Guest OS Type | Ubuntu (64-bit) |
| CPU | 2 |
| RAM | 2048 MB |
| DVD | ☑ |
| USB Controller | ☑ |
| Sound Card | ☑ ICH AC97 |
| Network Adapter | ☑ Intel PRO/1000 MT Desktop (82540EM) |
| Storage Controller (IDE) | PIIX4 |

☑ Reinitialize the MAC address of all network cards

Appliance is not signed

4. Wait while the appliance file is imported.



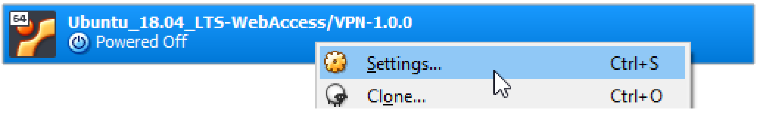
Importing Appliance ...: Importing appliance 'C:\Users\jan.svoboda\vpnport...

Importing virtual disk image 'vpnportal-standard-1-disk001.vmdk' ... (2/3)

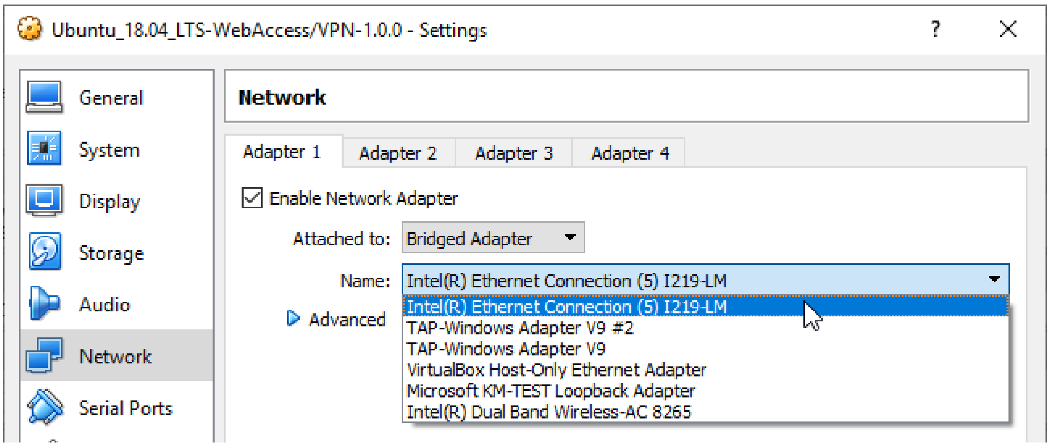
23%

52 seconds remaining

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.



Ubuntu_18.04_LTS-WebAccess/VPN-1.0.0 - Settings

Network

Adapter 1

☑ Enable Network Adapter

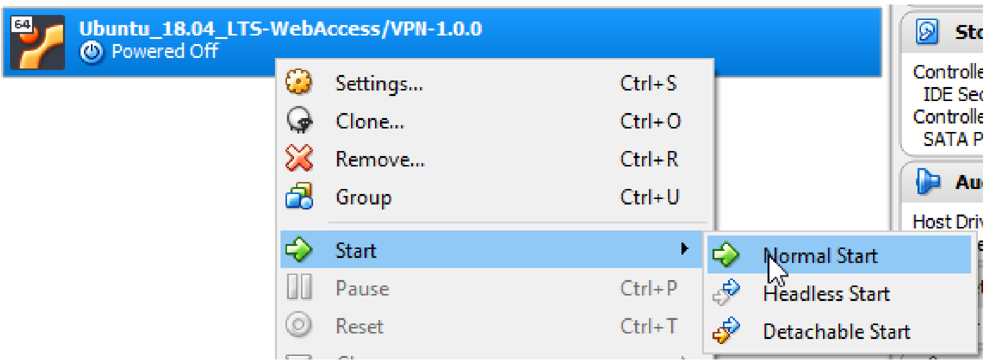
Attached to: Bridged Adapter

Name: Intel(R) Ethernet Connection (5) I219-LM

Intel(R) Ethernet Connection (5) I219-LM
TAP-Windows Adapter V9 #2
TAP-Windows Adapter V9
VirtualBox Host-Only Ethernet Adapter
Microsoft KM-TEST Loopback Adapter
Intel(R) Dual Band Wireless-AC 8265

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.

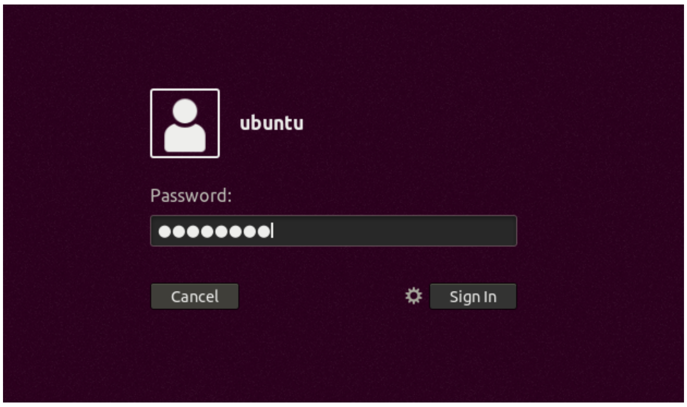
7. Now run the appliance:



Ubuntu_18.04_LTS-WebAccess/VPN-1.0.0
Powered Off

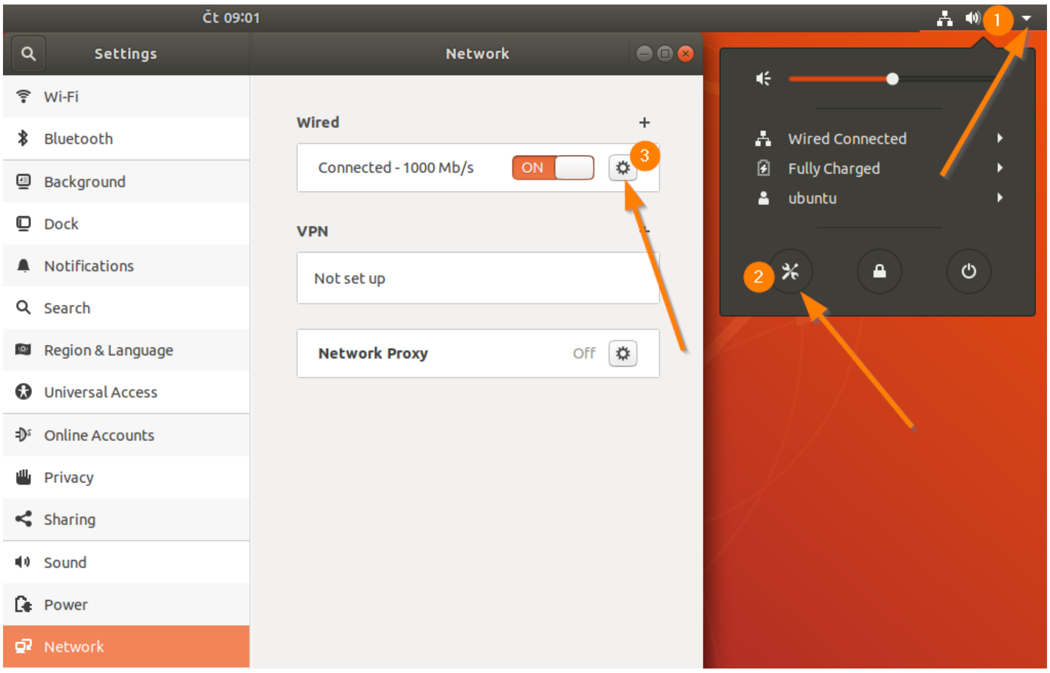
8. Wait for the system to boot and login to Ubuntu with these credentials:

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

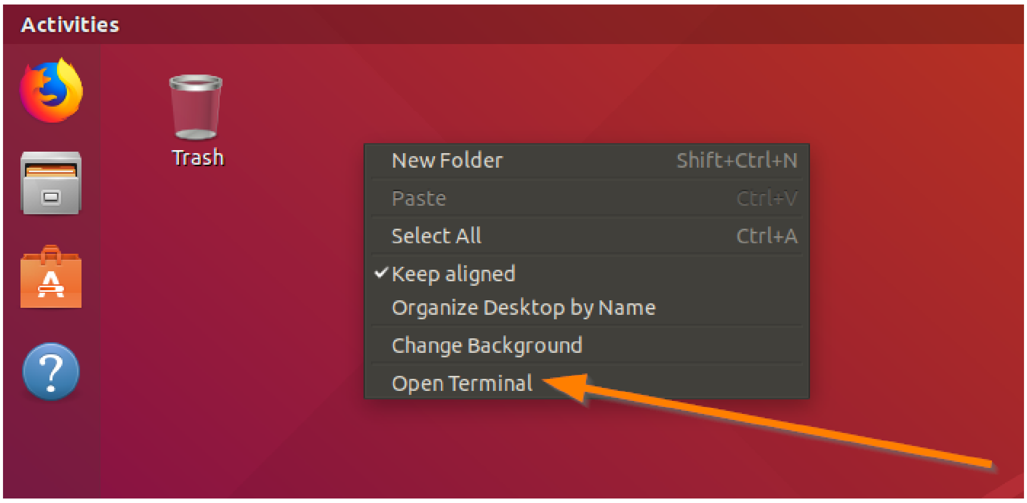


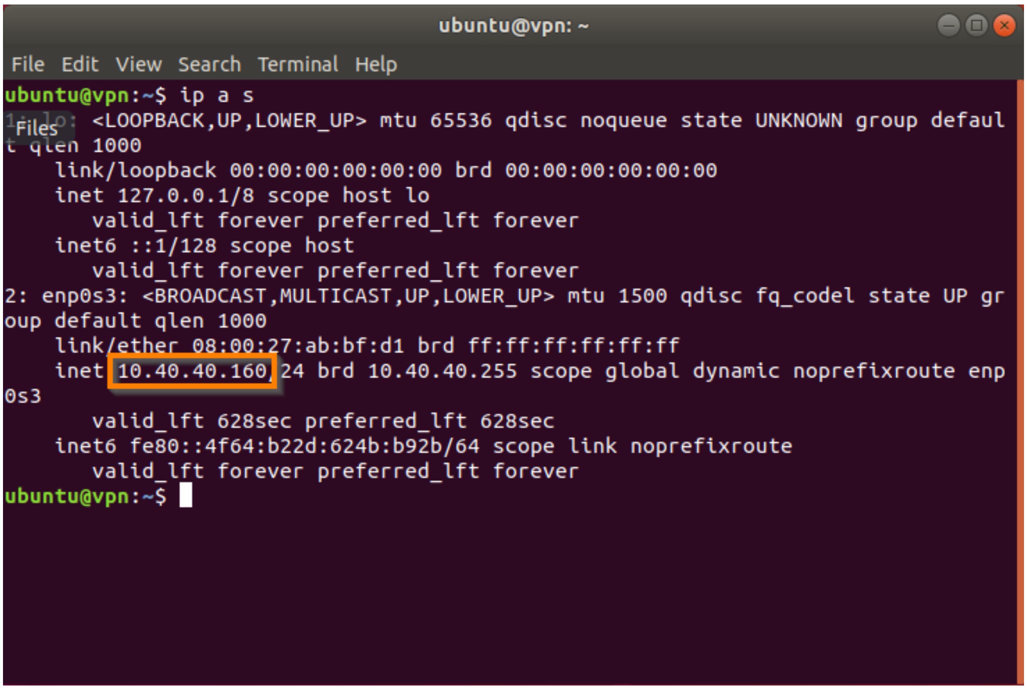
9. Find out the IP address of the appliance's bridged network interface. It is accessible either via GUI in system settings, or in terminal after a command prompt. Both methods are described below:

   **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 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).

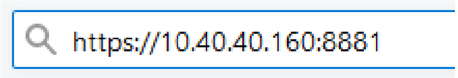




```
ubuntu@vpn:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:ab:bf:d1 brd ff:ff:ff:ff:ff:ff
    inet 10.40.40.160/24 brd 10.40.40.255 scope global dynamic noprefixroute enp
0s3
       valid_lft 628sec preferred_lft 628sec
    inet6 fe80::4f64:b22d:624b:b92b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
ubuntu@vpn:~$
```

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

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

    https://10.40.40.160:8881

    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).

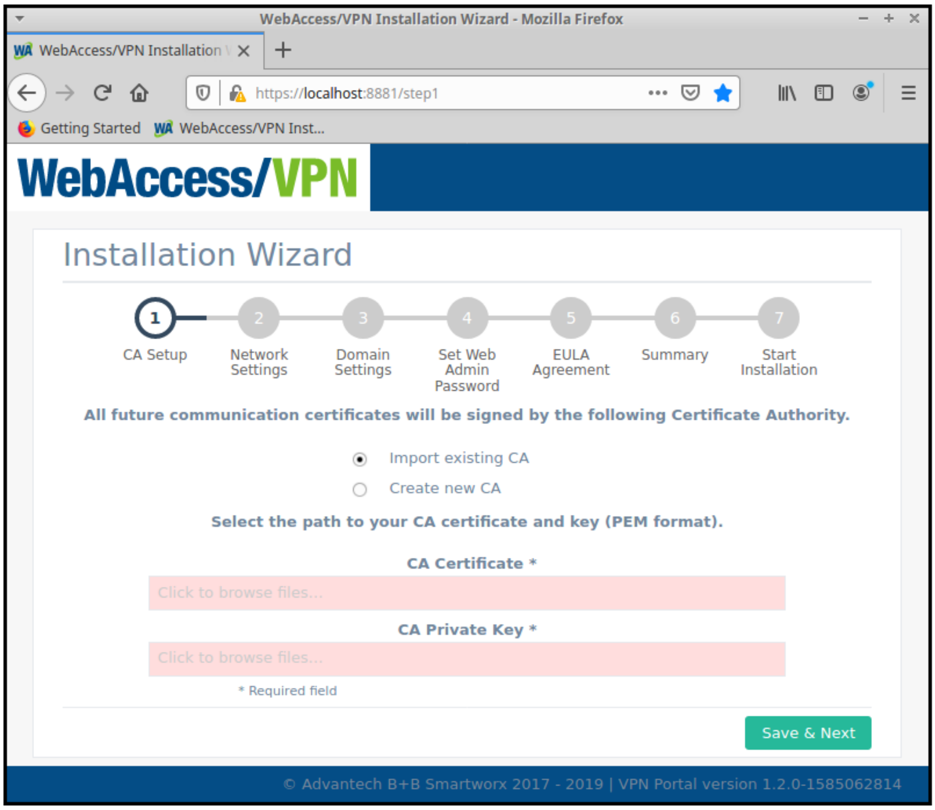
11. Continue in wizard, go to 2.5

## 2.4 VPN-BOX-UNO Installation

The *VPN-BOX-UNO23* product is an Advantech Embedded Automation Computer UNO-2372G with pre-installed *WebAccess/VPN* software acts as the *WebAccess/VPN* server.

There is a proprietary Advantech Linux distribution, based on the Xubuntu, installed on this computer.

1. Connect the *VPN-BOX-UNO23* device to power supply and to all the peripherals, see printed Start Guide for the details.
2. When the device boots up, the login screen should appear. Log in as **ubuntu** user with password **wavpn123**.
3. Click the *Web Browser* icon on the desktop and the *Mozilla Firefox* web browser will be opened.
4. Enter `https://localhost:8881` address or click on the shortcut in the *Bookmarks Menu*.
5. The first page of the *WebAccess/VPN* Installation Wizard should pop up.



Installation Wizard

All future communication certificates will be signed by the following Certificate Authority.

● Import existing CA

○ Create new CA

Select the path to your CA certificate and key (PEM format).

CA Certificate *

Click to browse files...

CA Private Key *

Click to browse files...

* Required field

© Advantech B+B Smartworx 2017 - 2019 | VPN Portal version 1.2.0-1585062814

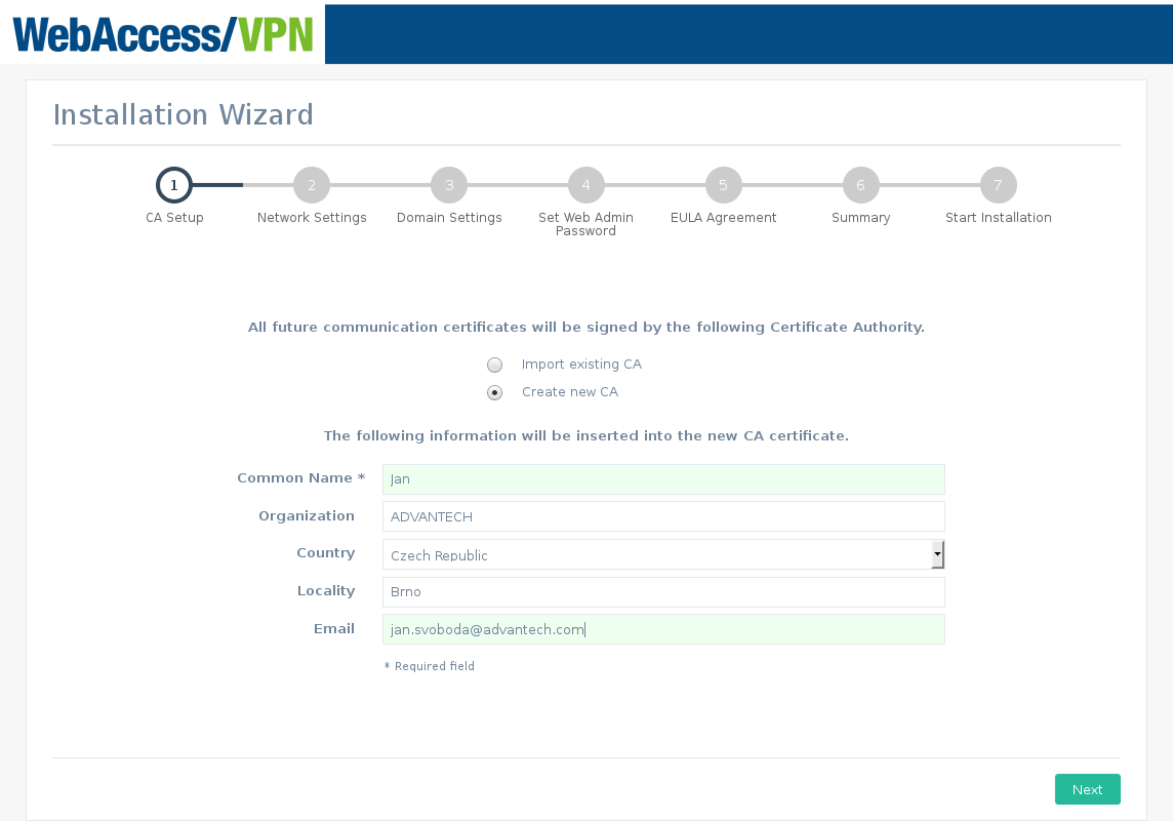
6. Continue with the configuration in the wizard, see chapter 2.5.

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

## 2.5 Installation Wizard

1. Follow the instructions in 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!



All future communication certificates will be signed by the following Certificate Authority.

○ Import existing CA

● Create new CA

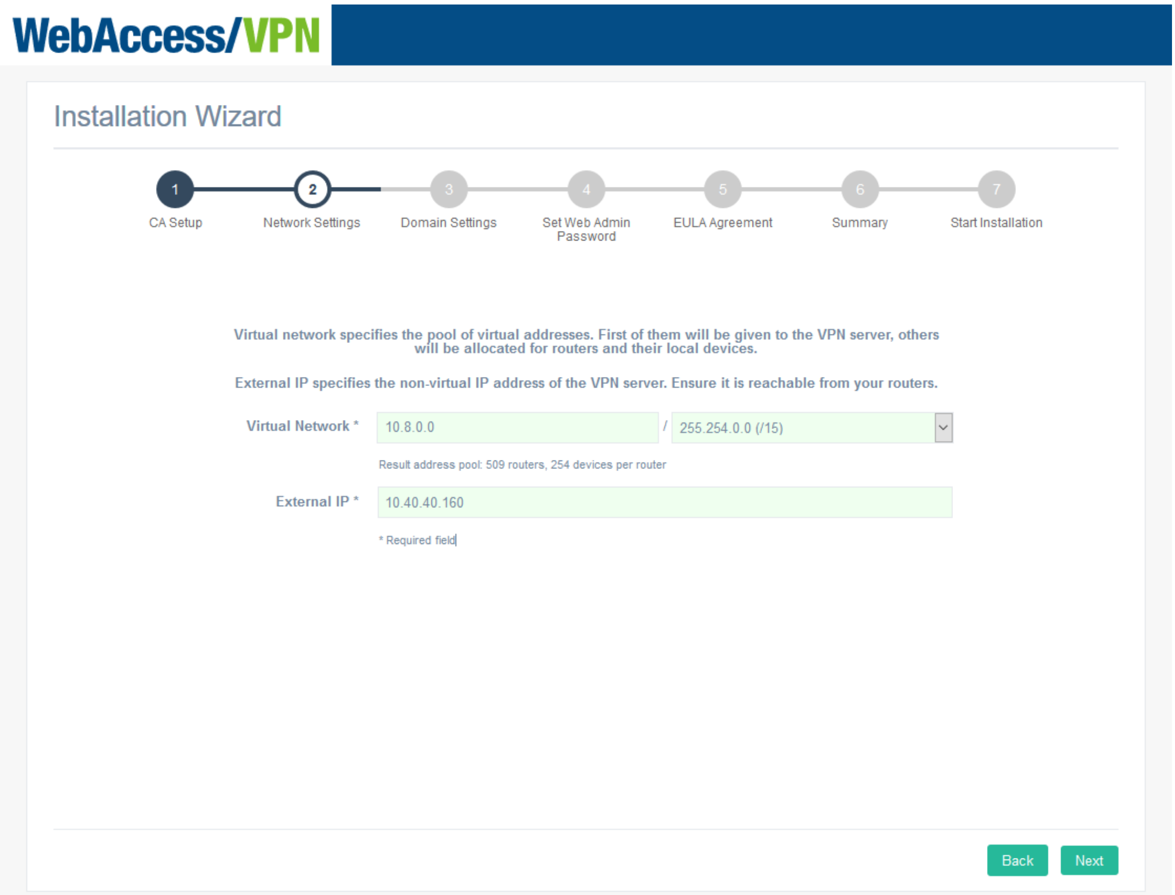
The following information will be inserted into the new CA certificate.

| | |
|---|---|
| Common Name * | Jan |
| Organization | ADVANTECH |
| Country | Czech Republic |
| Locality | Brno |
| Email | jan.svoboda@advantech.com |

* Required field

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. Number of devices per router is always 254 and can not be changed. Virtual network address and mask (affecting overall number of devices) can be changed later in setting, but only if there are no validated routers.

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



Virtual network specifies the pool of virtual addresses. First of them will be given to the VPN server, others will be allocated for routers and their local devices.

External IP specifies the non-virtual IP address of the VPN server. Ensure it is reachable from your routers.

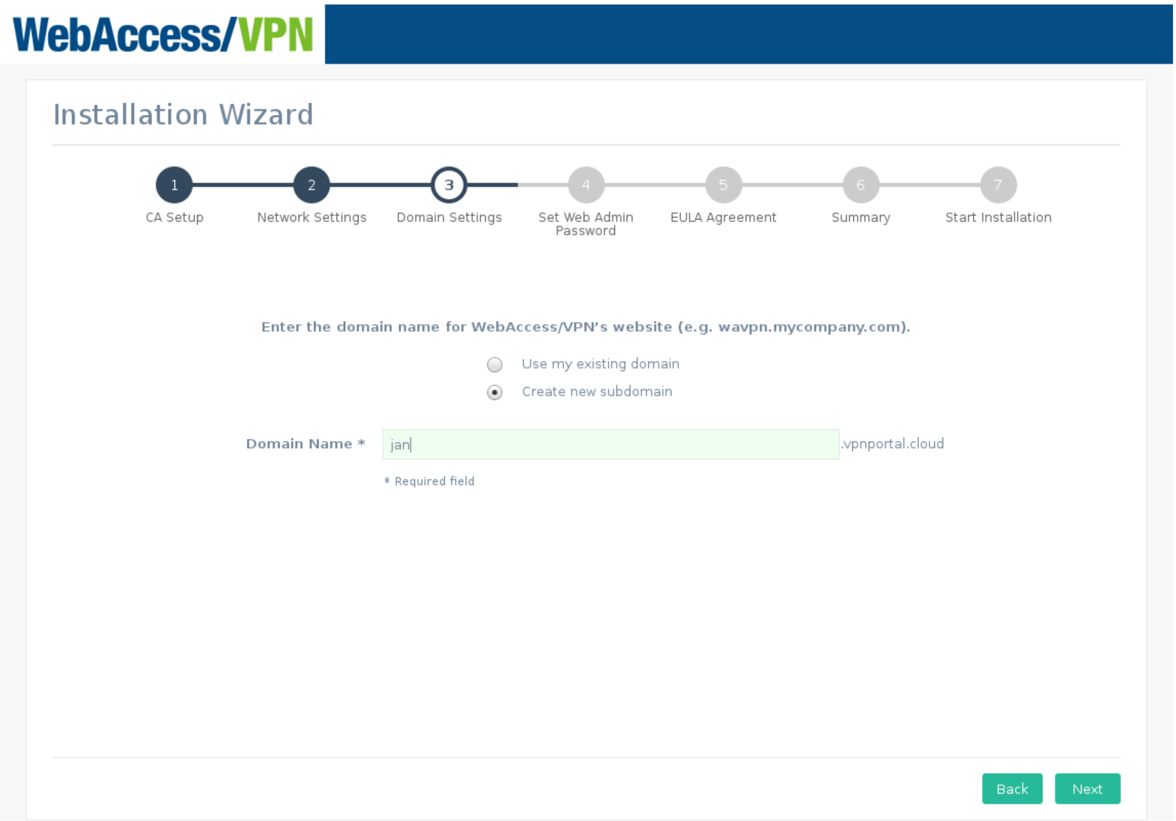
Virtual Network * 10.8.0.0 / 255.254.0.0 (/15)

Result address pool: 509 routers, 254 devices per router

External IP * 10.40.40.160

* Required field

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).



Enter the domain name for WebAccess/VPN's website (e.g. wavpn.mycompany.com).

○ Use my existing domain
● Create new subdomain

Domain Name * jan .vpnportal.cloud

* Required field

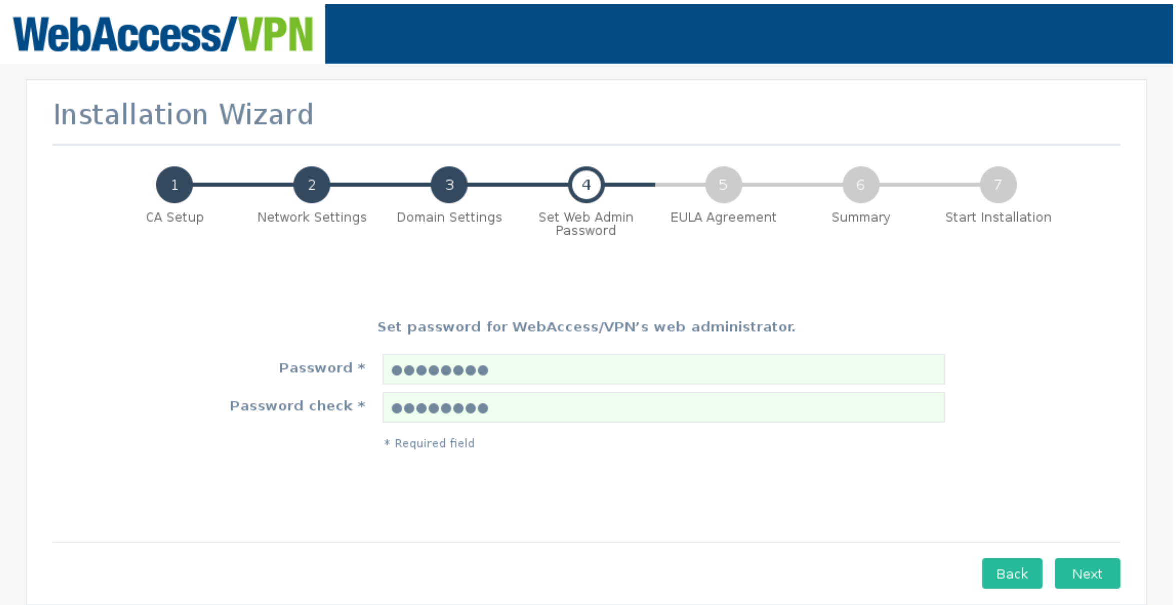
**Warning:** On AWS, do not use your instance DNS domain name
(e. g. ec2-35-156-197-5.eu-central-1.compute.amazonaws.com).

Note that the AWS instance may change its public IP when stopped and run again, so either do 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 it would be with your own domain.

4. In step 4, setup the password for Web user admin access.



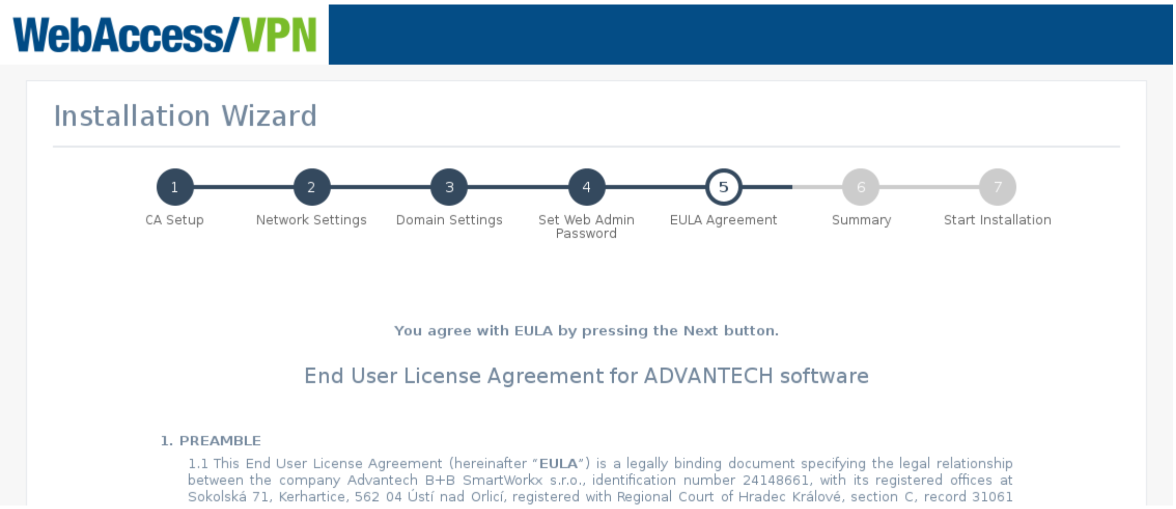
Set password for WebAccess/VPN's web administrator.

Password * ●●●●●●●●

Password check * ●●●●●●●●

* Required field

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



You agree with EULA by pressing the Next button.

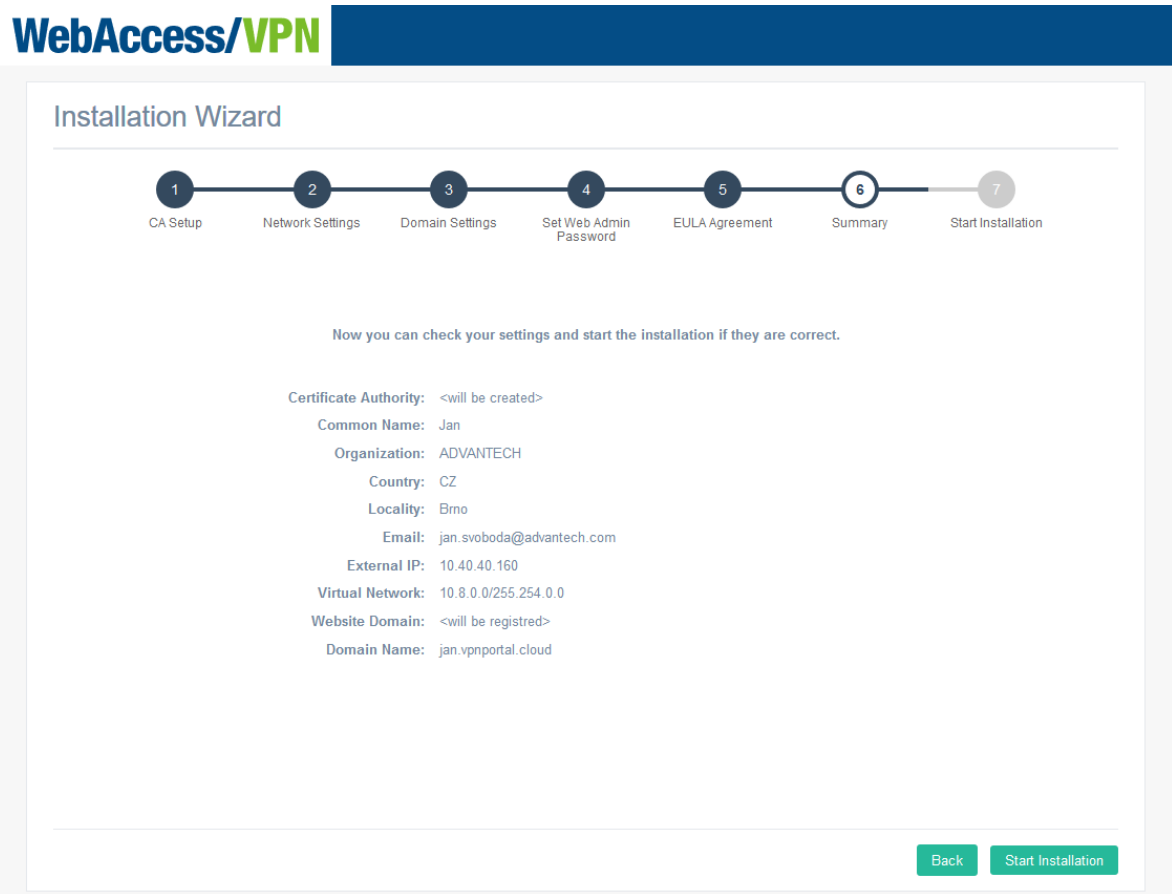
End User License Agreement for ADVANTECH software

1. PREAMBLE

1.1 This End User License Agreement (hereinafter "**EULA**") is a legally binding document specifying the legal relationship between the company Advantech B+B SmartWorkx s.r.o., identification number 24148661, with its registered offices at Sokolská 71, Kerhartice, 562 04 Ústí nad Orlicí, registered with Regional Court of Hradec Králové, section C, record 31061

6. In step 6, check the installation parameters.

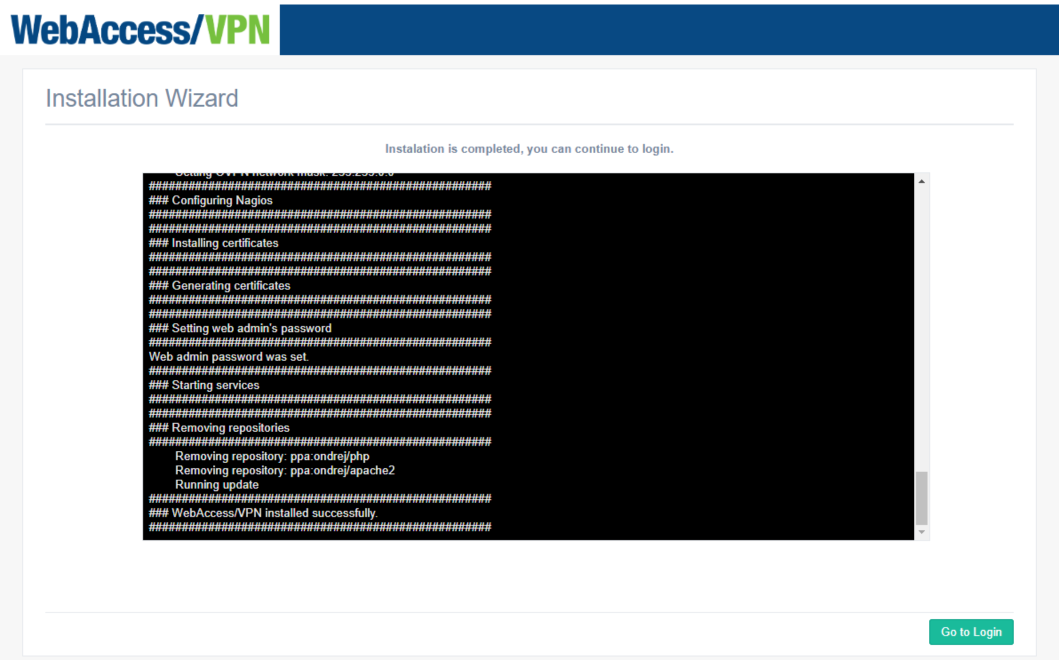
! Note that the installation wizard can be run only once and will be deactivated after the installation.



Now you can check your settings and start the installation if they are correct.

| | |
|---|---|
| Certificate Authority: | <will be created> |
| Common Name: | Jan |
| Organization: | ADVANTECH |
| Country: | CZ |
| Locality: | Brno |
| Email: | jan.svoboda@advantech.com |
| External IP: | 10.40.40.160 |
| Virtual Network: | 10.8.0.0/255.254.0.0 |
| Website Domain: | <will be registred> |
| Domain Name: | jan.vpnportal.cloud |

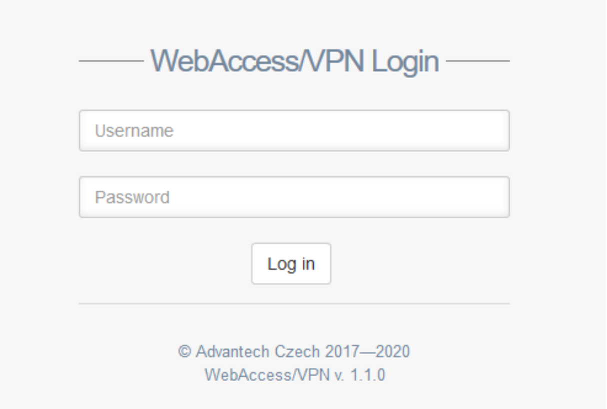
7. Click *Start installation*. There will be progress bar showing the status of the installation. After the installation is done, the message "Installation is completed, you can continue to login" will appear and the button *Go to Login* will be active.



Instalation is completed, you can continue to login.

```
    Setting OVPN network mask: 255.255.0.0
############################################################
### Configuring Nagios
############################################################
############################################################
### Installing certificates
############################################################
############################################################
### Generating certificates
############################################################
############################################################
### Setting web admin's password
############################################################
Web admin password was set.
############################################################
### Starting services
############################################################
############################################################
### Removing repositories
############################################################
      Removing repository: ppa:ondrej/php
      Removing repository: ppa:ondrej/apache2
      Running update
############################################################
### WebAccess/VPN installed successfully.
############################################################
```

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.



© Advantech Czech 2017—2020
WebAccess/VPN v. 1.1.0

The default license described in Chapter 1.3 is active after installation. You can download router user modules 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

For production use we recommend to choose an instance with at least 2 CPUs and 4 GB of RAM. 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 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.)

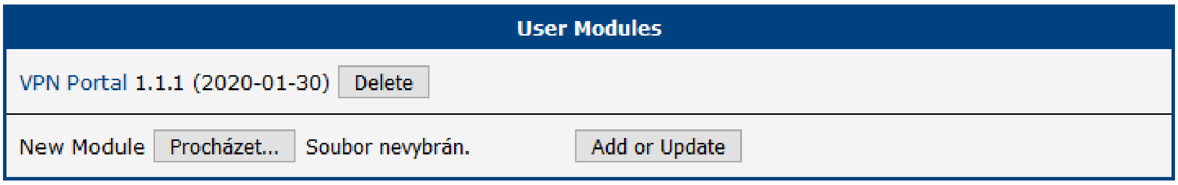
- Currently OpenVPN is not capable of using more than 1 CPU core, so more CPU cores does not help with traffic in this case. Thus 2 CPU cores will be sufficient for most applications (1 for OpenVPN and 1 for the rest).

# 3. Configuration of Advantech Router

## 3.1 Upload User Module VPN Portal

Upload the user module *VPN Portal* to the router to connect the router to WebAccess/VPN. It can be done on the *User Modules* page in the router's Web interface.

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



User Modules

VPN Portal 1.1.1 (2020-01-30) Delete

New Module Procházet... Soubor nevybrán. Add or Update

Figure 5: User module *VPN Portal* after upload to the router

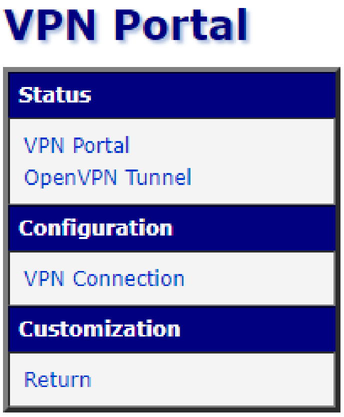


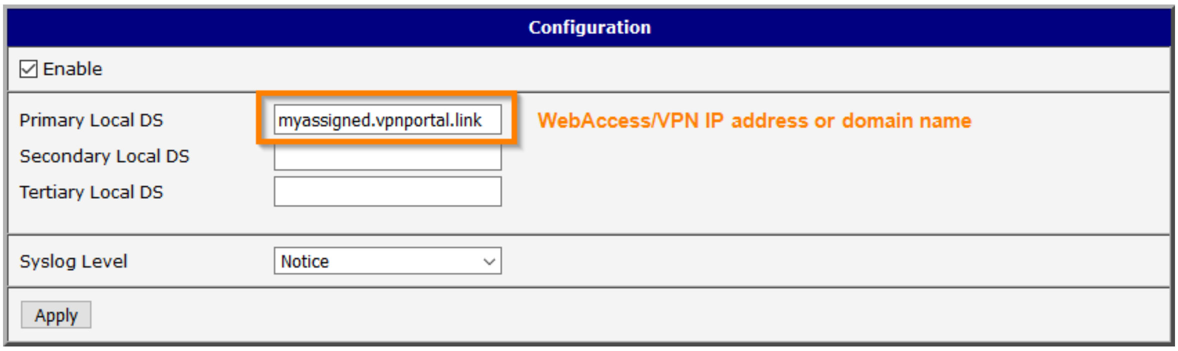
Figure 6: User module menu

The Web interface of the user module is accessible by clicking on the user module'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 Web interface of the router using the *Return* button in the *Customization* section.

## 3.2 Connect the Router to WebAccess/VPN

Make sure that 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. Make sure 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 cloud) so just fill in your WebAccess/VPN IP address or domain name into *Primary Local DS* field. Secondary and Tretiary DS fields are not mandatory.


Configuration

☑ Enable

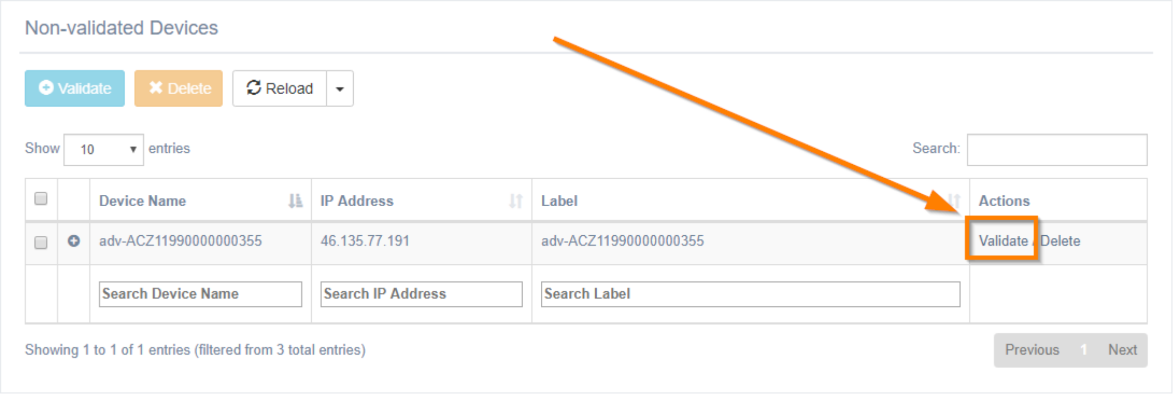
| | |
|---|---|
| Primary Local DS | myassigned.vpnportal.link |
| Secondary Local DS | |
| Tertiary Local DS | |
| Syslog Level | Notice |

Figure 7: *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 enables the possibility to run 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 8:



| ☐ | | Device Name | IP Address | Label | Actions |
|---|---|---|---|---|---|
| ☐ | ⊕ | adv-ACZ11990000000355 | 46.135.77.191 | adv-ACZ11990000000355 | Validate / Delete |
| | | Search Device Name | Search IP Address | Search Label | |

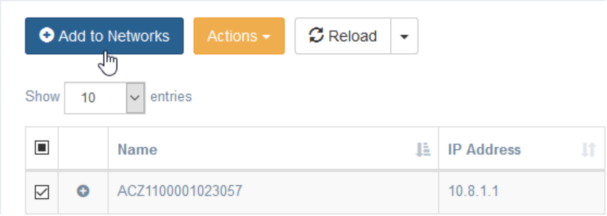
Showing 1 to 1 of 1 entries (filtered from 3 total entries)

Figure 8: Validating the router in WebAccess/VPN Web UI

## 3.4 Set the Router Access Policy

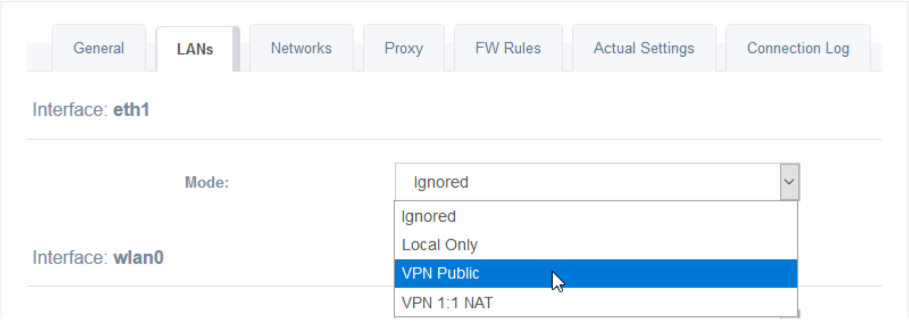
By validating routers to WebAccess/VPN, they do not see each other automatically.

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



| ▣ | | Name | IP Address |
|---|---|---|---|
| ☑ | ⊕ | ACZ1100001023057 | 10.8.1.1 |

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



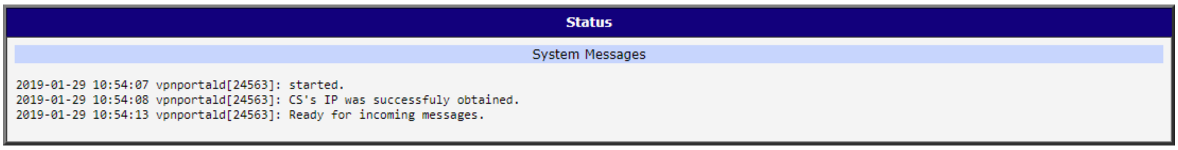
Interface: **eth1**

Mode: Ignored

Interface: **wlan0**

## 3.5 User Module Status and Log Messages

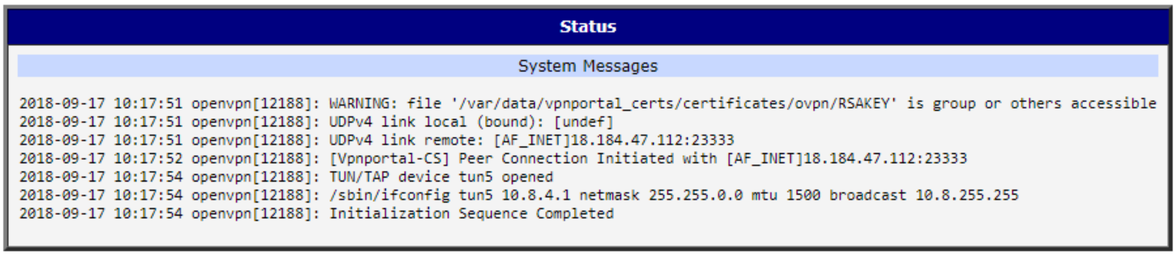
After the router is validated in WebAccess/VPN Web UI, you can see the "`Ready for incoming messages`" notice on *VPN Portal* status page in the router:



```
2019-01-29 10:54:07 vpnportald[24563]: started.
2019-01-29 10:54:08 vpnportald[24563]: CS's IP was successfuly obtained.
2019-01-29 10:54:13 vpnportald[24563]: Ready for incoming messages.
```

Figure 9: *VPN Portal* status page of the validated router

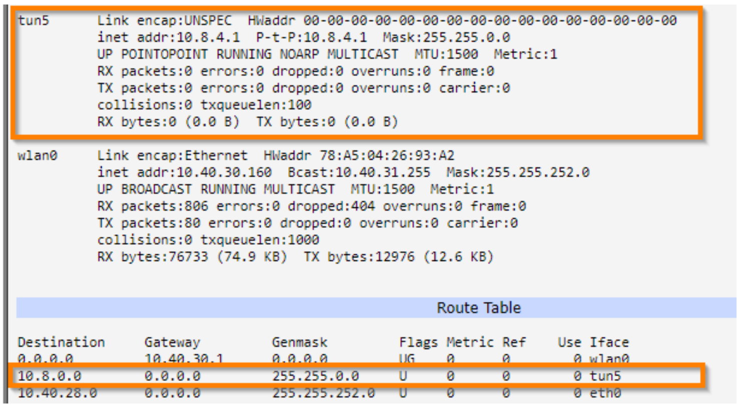
Also on the *OpenVPN Tunnel* page there will be "`Initialization Sequence Completed`" notice if the tunnel establishment is successful:



```
2018-09-17 10:17:51 openvpn[12188]: WARNING: file '/var/data/vpnportal_certs/certificates/ovpn/RSAKEY' is group or others accessible
2018-09-17 10:17:51 openvpn[12188]: UDPv4 link local (bound): [undef]
2018-09-17 10:17:51 openvpn[12188]: UDPv4 link remote: [AF_INET]18.184.47.112:23333
2018-09-17 10:17:52 openvpn[12188]: [Vpnportal-CS] Peer Connection Initiated with [AF_INET]18.184.47.112:23333
2018-09-17 10:17:54 openvpn[12188]: TUN/TAP device tun5 opened
2018-09-17 10:17:54 openvpn[12188]: /sbin/ifconfig tun5 10.8.4.1 netmask 255.255.0.0 mtu 1500 broadcast 10.8.255.255
2018-09-17 10:17:54 openvpn[12188]: Initialization Sequence Completed
```

Figure 10: *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:



```
tun5      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.4.1  P-t-P:10.8.4.1  Mask:255.255.0.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  HWaddr 78:A5:04:26:93:A2
          inet addr:10.40.30.160  Bcast:10.40.31.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:806 errors:0 dropped:404 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76733 (74.9 KB)  TX bytes:12976 (12.6 KB)
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.40.30.1      0.0.0.0         UG    0      0        0 wlan0
10.8.0.0        0.0.0.0         255.255.0.0     U     0      0        0 tun5
10.40.28.0      0.0.0.0         255.255.252.0   U     0      0        0 eth0
```

Figure 11: 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. 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 User Module Log Messages

The user module 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 user module received the necessary address and now it can move to the next phase.

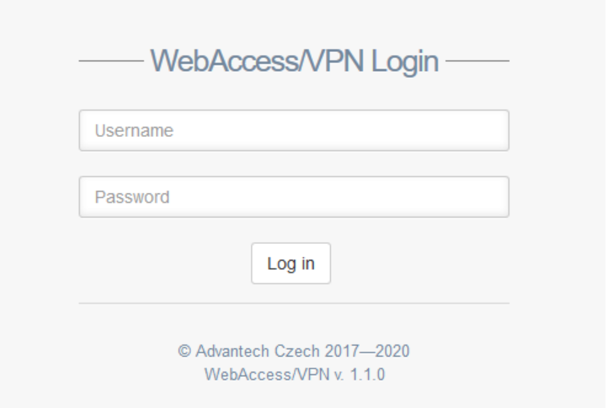
If the router obtained the Customer Server's (CS) IP address, it will contact the CS to ask to be allowed into the WebAccess/VPN network. There are 3 possible outcomes:

- *"Failed to connect to the Customer Server."* – The Customer Server is unreachable or stopped.
- *"Negative response to request for OVPN certificates."* – The router hasn't been validated on Customer Server, yet.
- *"Ready for incoming messages"* – Tunnel between router and Customer Server has been established. From now on, 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

The Web user interface of WebAccess/VPN (CS) is running on the server after the installation. Navigate your browser to the server and login:

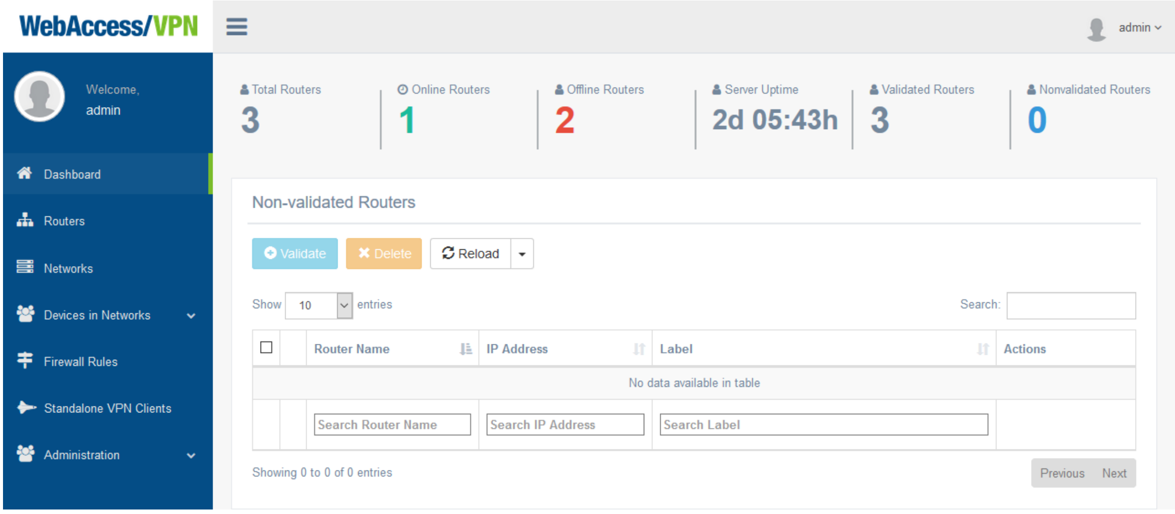


© Advantech Czech 2017—2020
WebAccess/VPN v. 1.1.0

Figure 12: Login to WebAccess/VPN

## 4.2 Dashboard

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



| Total Routers | Online Routers | Offline Routers | Server Uptime | Validated Routers | Nonvalidated Routers |
|---|---|---|---|---|---|
| 3 | 1 | 2 | 2d 05:43h | 3 | 0 |

Non-validated Routers

Show 10 entries Search:

| ☐ | Router Name | IP Address | Label | Actions |
|---|---|---|---|---|
| | No data available in table | | | |
| | Search Router Name | Search IP Address | Search Label | |

Showing 0 to 0 of 0 entries

Figure 13: 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*.

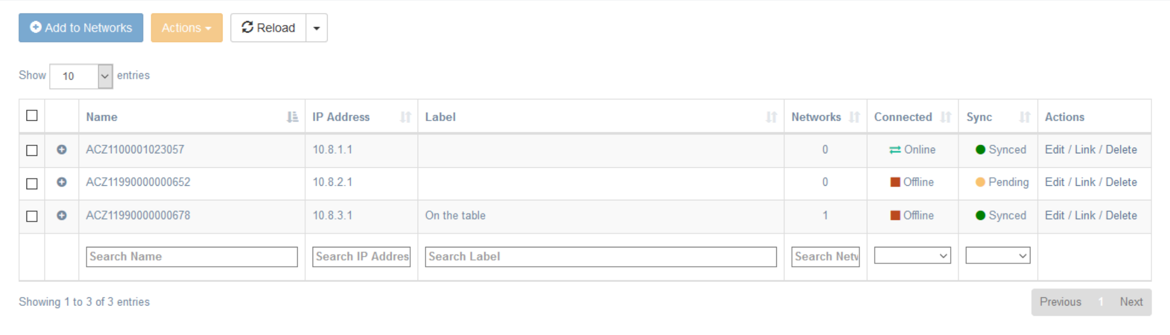
Th list of Non-validated routers is below the overview. Validate connected routers as shown in Figure 8. You can also delete routers you do not want to validate. You can do these actions in bulk using the checkboxes and buttons at the top of the devices list. This is the only place (on the Dashboard) 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 has to be added into a network and also 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 next 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 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 dropdown the *Reload* button. Router properties are explained in Table 1 below.



Show 10 entries

| ☐ | | Name | IP Address | Label | Networks | Connected | Sync | Actions |
|---|---|---|---|---|---|---|---|---|
| ☐ | ⊕ | ACZ1100001023057 | 10.8.1.1 | | 0 | ⇄ Online | ● Synced | Edit / Link / Delete |
| ☐ | ⊕ | ACZ11990000000652 | 10.8.2.1 | | 0 | ■ Offline | ● Pending | Edit / Link / Delete |
| ☐ | ⊕ | ACZ11990000000678 | 10.8.3.1 | On the table | 1 | ■ Offline | ● Synced | Edit / Link / Delete |
| | | Search Name | Search IP Addres | Search Label | Search Netv | | | |

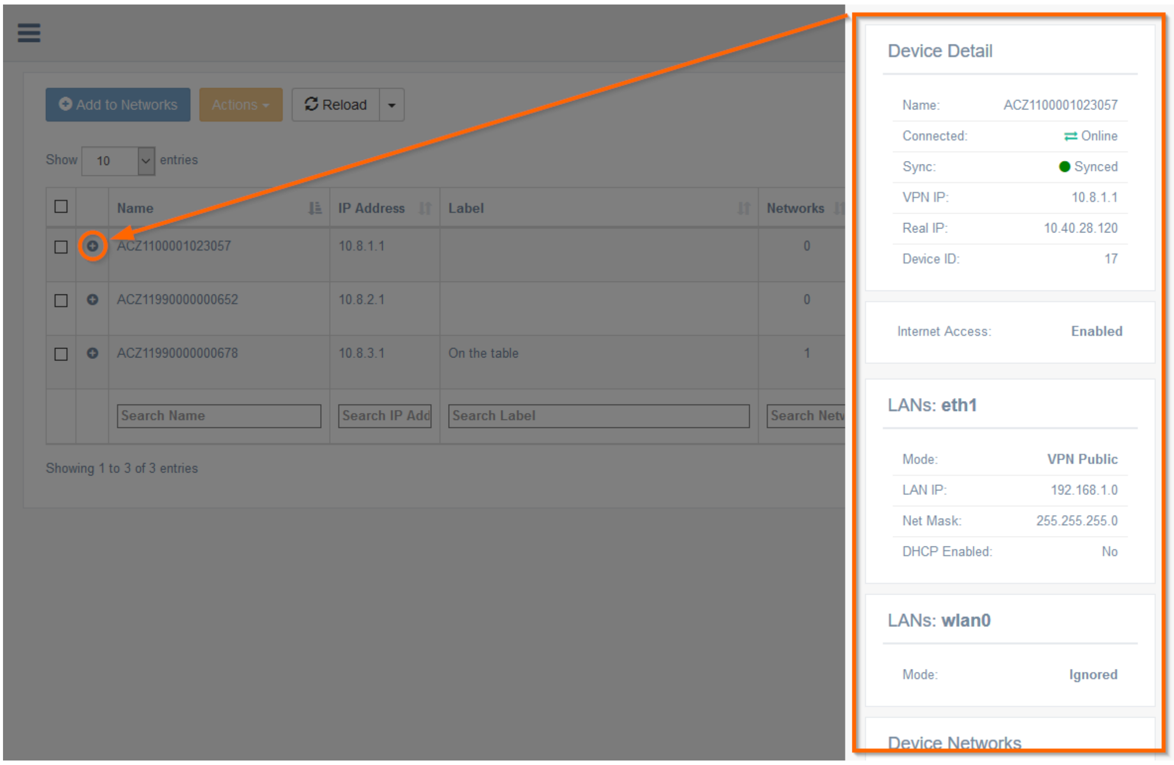
Showing 1 to 3 of 3 entries

Figure 14: Routers in WebAccess/VPN

| Router Property | Description |
|---|---|
| Name | An automatically obtained name of the Router. Based on Serial Number in most cases (if SN not available, 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 user module's log in the Router for details about the failure. |
| Actions | **Edit** – Access the main page of the Router with more information and further 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 15. 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.



Show 10 entries

| ☐ | | Name | IP Address | Label | Networks |
|---|---|---|---|---|---|
| ☐ | ⊕ | ACZ1100001023057 | 10.8.1.1 | | 0 |
| ☐ | ⊕ | ACZ11990000000652 | 10.8.2.1 | | 0 |
| ☐ | ⊕ | ACZ11990000000678 | 10.8.3.1 | On the table | 1 |
| | | Search Name | Search IP Add | Search Label | Search Netv |

Showing 1 to 3 of 3 entries

Device Detail

| | |
|---|---|
| Name: | ACZ1100001023057 |
| Connected: | ⇄ Online |
| Sync: | ● Synced |
| VPN IP: | 10.8.1.1 |
| Real IP: | 10.40.28.120 |
| Device ID: | 17 |

| | |
|---|---|
| Internet Access: | Enabled |

LANs: **eth1**

| | |
|---|---|
| Mode: | VPN Public |
| LAN IP: | 192.168.1.0 |
| Net Mask: | 255.255.255.0 |
| DHCP Enabled: | No |

LANs: **wlan0**

| | |
|---|---|
| Mode: | Ignored |

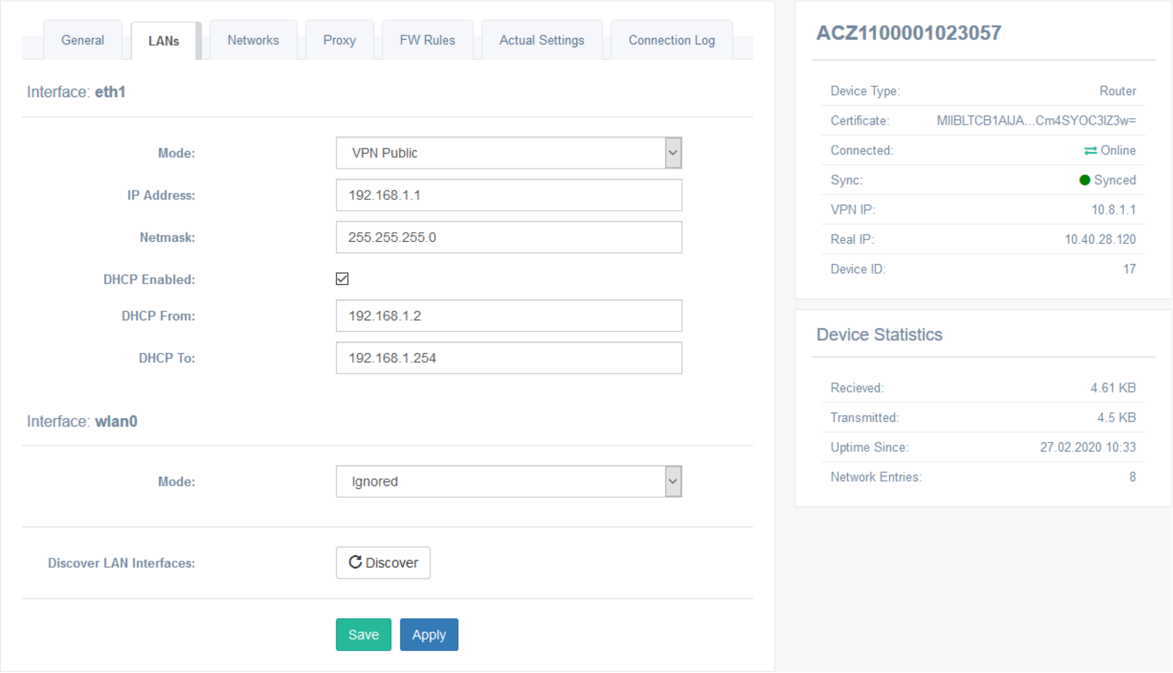
Device Networks

Figure 15: Routers – Overview of a Router

### 4.3.1 Routers: Edit

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

#### LANs Tab



Interface: **eth1**

Mode: VPN Public
IP Address: 192.168.1.1
Netmask: 255.255.255.0
DHCP Enabled: ☑
DHCP From: 192.168.1.2
DHCP To: 192.168.1.254

Interface: **wlan0**

Mode: Ignored

Discover LAN Interfaces:

**ACZ1100001023057**

| | |
|---|---|
| Device Type: | Router |
| Certificate: | MIIBLTCB1AIJA...Cm4SYOC3IZ3w= |
| Connected: | ⇄ Online |
| Sync: | ● Synced |
| VPN IP: | 10.8.1.1 |
| Real IP: | 10.40.28.120 |
| Device ID: | 17 |

**Device Statistics**

| | |
|---|---|
| Recieved: | 4.61 KB |
| Transmitted: | 4.5 KB |
| Uptime Since: | 27.02.2020 10:33 |
| Network Entries: | 8 |

Figure 16: Routers – main page of a Router – Edit LANs

| Interface Mode | Description |
|---|---|
| Ignored | Customer Server is not managing the Router‘s LAN. |
| Local Only | Administrator is able to 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 is able to configure the LAN and it is made 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 16 |
| 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. |

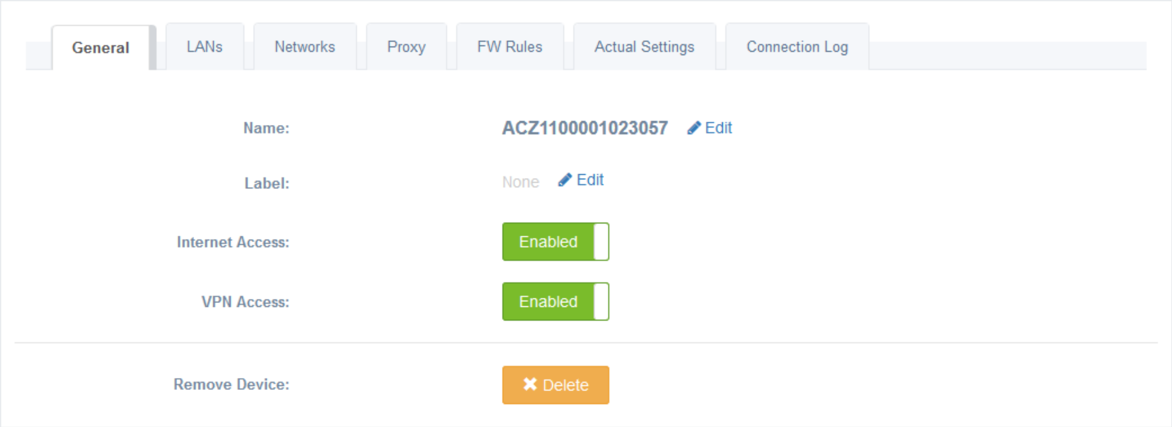
Table 2: Devices – LANs Interface Modes

**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 there was an interface change on the Router (e.g. Backup Routes configuration was changed on the Router) and you want to scan again the interfaces 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



Name: ACZ1100001023057

Label: None

Internet Access: Enabled

VPN Access: Enabled

Remove Device: Delete

Figure 17: Routers – General tab of a Router

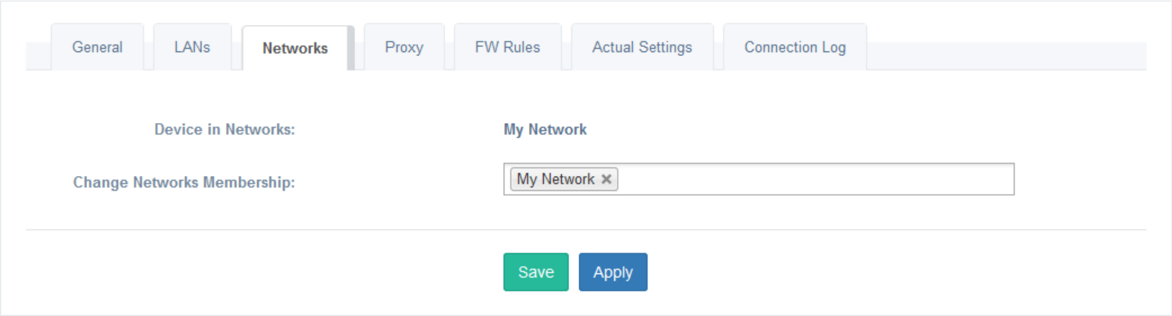
**Name, Label:** Rename the Router or change the Label by *Edit* link with pencil icon.

**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 Pending state if it is Offline, or Disabled. The actual state of 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 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, it will take effect immediately. 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). To add the device again in future, the validation process has to be repeated.

### Networks Tab



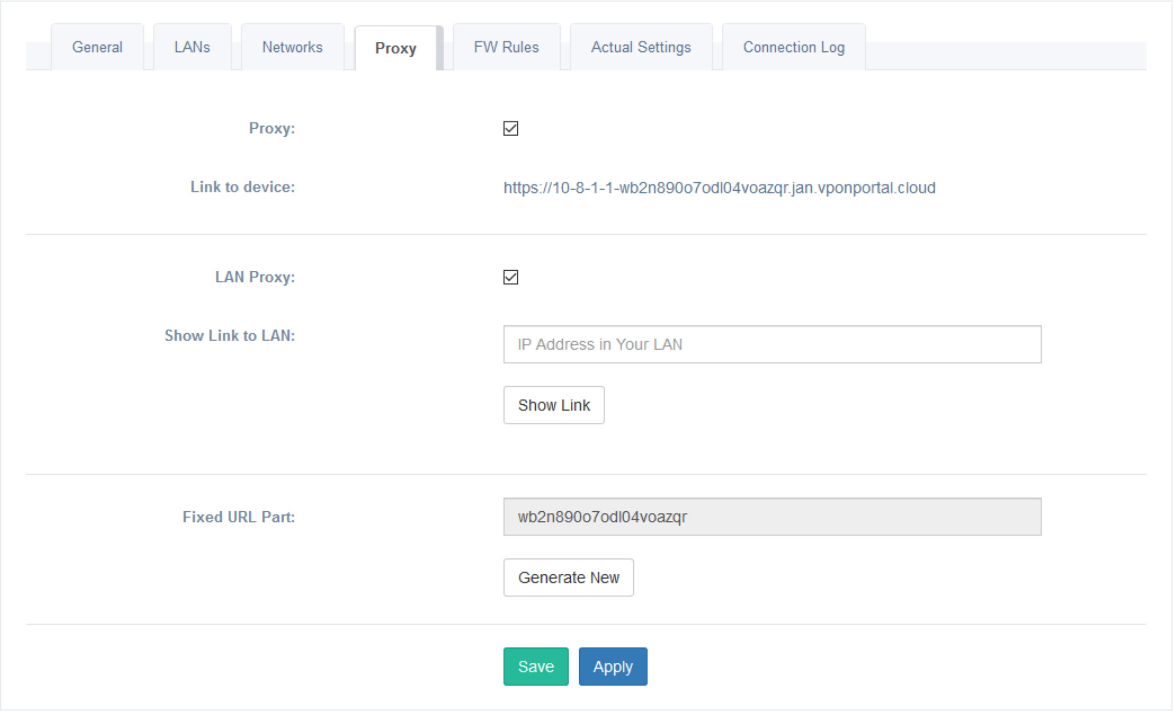
Device in Networks: My Network

Change Networks Membership: My Network ×

Figure 18: Routers – Networks membership of a Router

You can add a Router into 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



Proxy: ☑

Link to device: https://10-8-1-1-wb2n890o7odl04voazqr.jan.vponportal.cloud

LAN Proxy: ☑

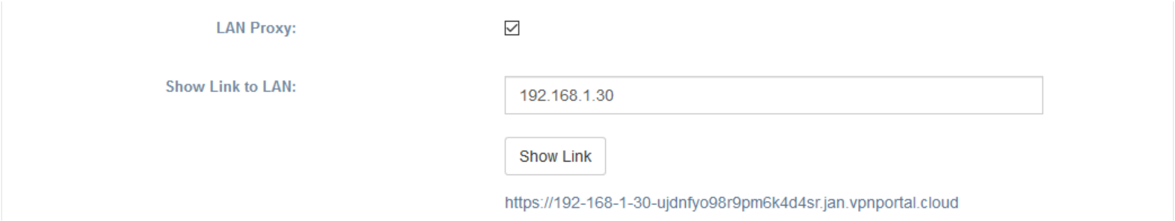
Show Link to LAN: IP Address in Your LAN

Fixed URL Part: wb2n890o7odl04voazqr

Figure 19: 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 (this is 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 address creator below the checkbox to see the link to your device. Fill in your device local IP address and click *Show Link* button.



LAN Proxy: ☑

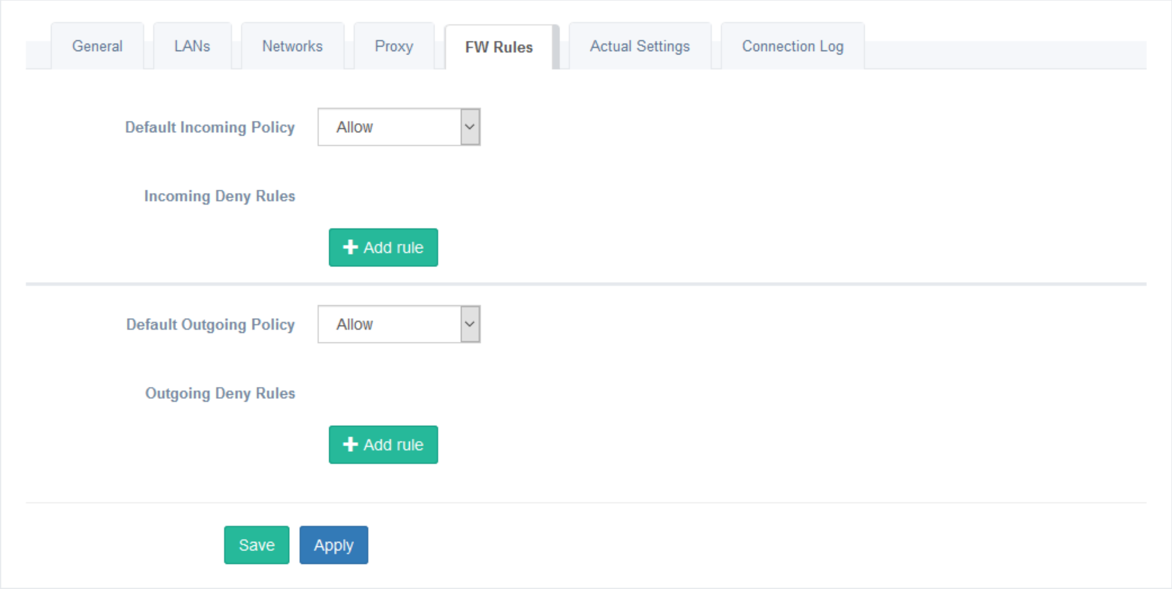
Show Link to LAN: 192.168.1.30

https://192-168-1-30-ujdnfyo98r9pm6k4d4sr.jan.vpnportal.cloud

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



Default Incoming Policy: Allow

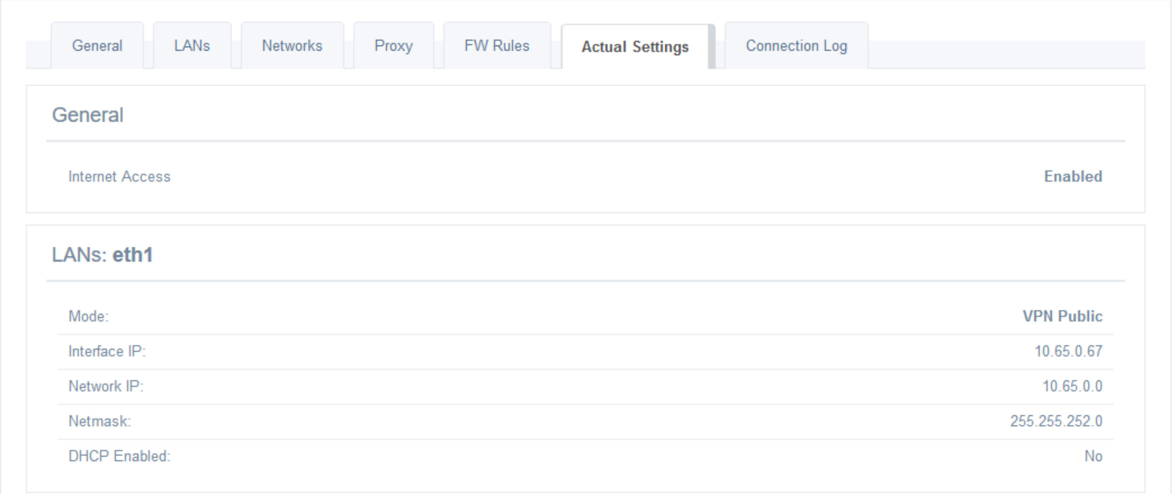
Default Outgoing Policy: Allow

Figure 20: 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



General

|  |  |
|---|---|
| Internet Access | Enabled |

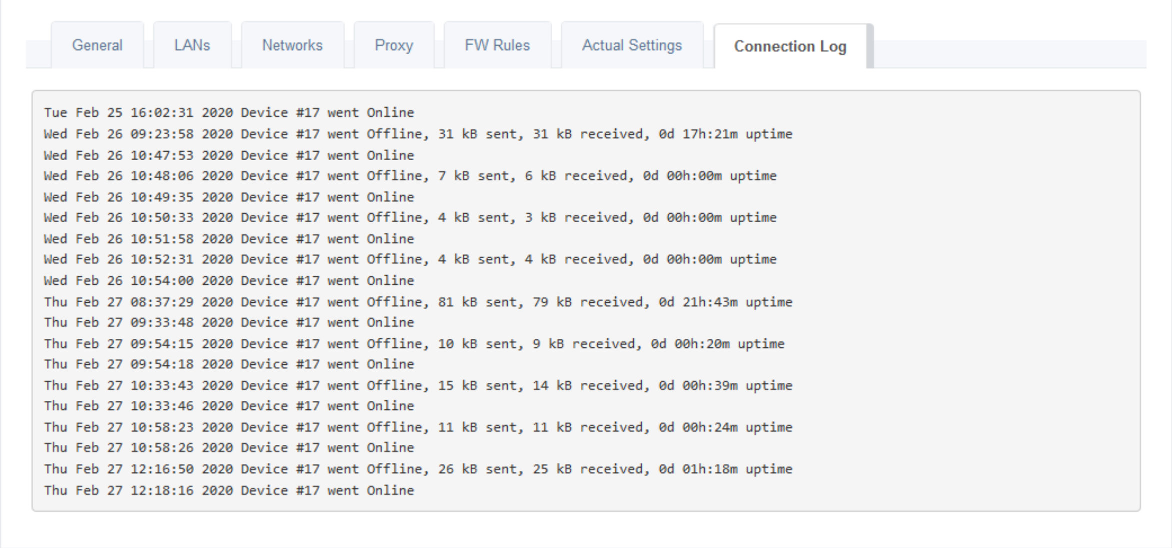
LANs: eth1

|  |  |
|---|---|
| Mode: | VPN Public |
| Interface IP: | 10.65.0.67 |
| Network IP: | 10.65.0.0 |
| Netmask: | 255.255.252.0 |
| DHCP Enabled: | No |

Figure 21: Routers – Actual Settings of a Router

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

### Connection Log Tab



```
Tue Feb 25 16:02:31 2020 Device #17 went Online
Wed Feb 26 09:23:58 2020 Device #17 went Offline, 31 kB sent, 31 kB received, 0d 17h:21m uptime
Wed Feb 26 10:47:53 2020 Device #17 went Online
Wed Feb 26 10:48:06 2020 Device #17 went Offline, 7 kB sent, 6 kB received, 0d 00h:00m uptime
Wed Feb 26 10:49:35 2020 Device #17 went Online
Wed Feb 26 10:50:33 2020 Device #17 went Offline, 4 kB sent, 3 kB received, 0d 00h:00m uptime
Wed Feb 26 10:51:58 2020 Device #17 went Online
Wed Feb 26 10:52:31 2020 Device #17 went Offline, 4 kB sent, 4 kB received, 0d 00h:00m uptime
Wed Feb 26 10:54:00 2020 Device #17 went Online
Thu Feb 27 08:37:29 2020 Device #17 went Offline, 81 kB sent, 79 kB received, 0d 21h:43m uptime
Thu Feb 27 09:33:48 2020 Device #17 went Online
Thu Feb 27 09:54:15 2020 Device #17 went Offline, 10 kB sent, 9 kB received, 0d 00h:20m uptime
Thu Feb 27 09:54:18 2020 Device #17 went Online
Thu Feb 27 10:33:43 2020 Device #17 went Offline, 15 kB sent, 14 kB received, 0d 00h:39m uptime
Thu Feb 27 10:33:46 2020 Device #17 went Online
Thu Feb 27 10:58:23 2020 Device #17 went Offline, 11 kB sent, 11 kB received, 0d 00h:24m uptime
Thu Feb 27 10:58:26 2020 Device #17 went Online
Thu Feb 27 12:16:50 2020 Device #17 went Offline, 26 kB sent, 25 kB received, 0d 01h:18m uptime
Thu Feb 27 12:18:16 2020 Device #17 went Online
```

Figure 22: Routers – Connection Log of a Router

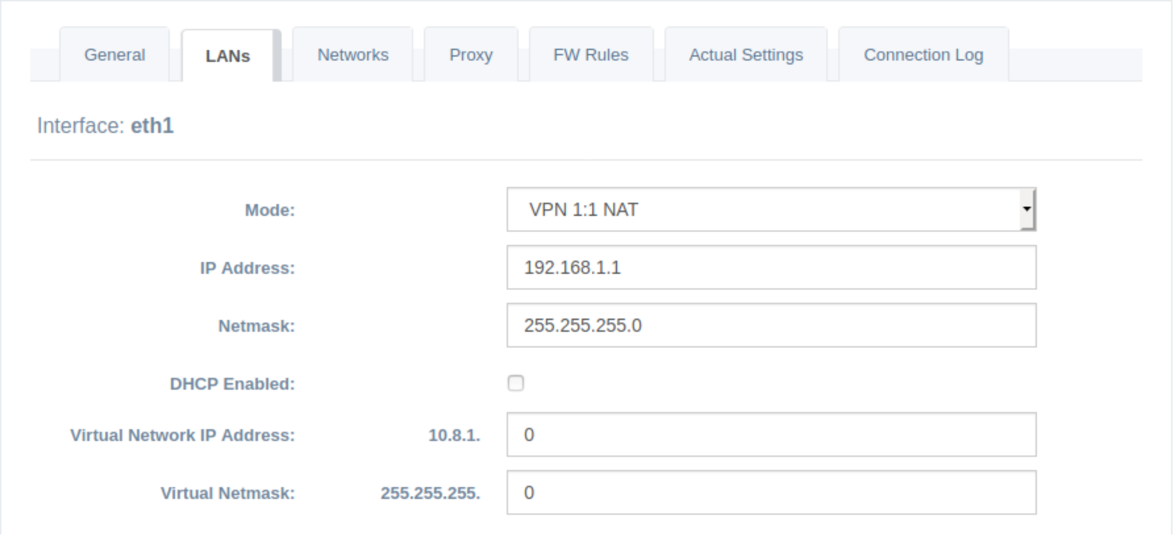
View the connection logs for the Router. This is filtered overall Connection Log accessible in *Administration* – Logs.

### 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 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:



Interface: **eth1**

Mode: VPN 1:1 NAT

IP Address: 192.168.1.1

Netmask: 255.255.255.0

DHCP Enabled: □

Virtual Network IP Address: 10.8.1. 0

Virtual Netmask: 255.255.255. 0

Figure 23: 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 Customer Server:

- Virtual IP of the first router is 10.8.1.1, 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, 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 performs the translation of 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 ...).

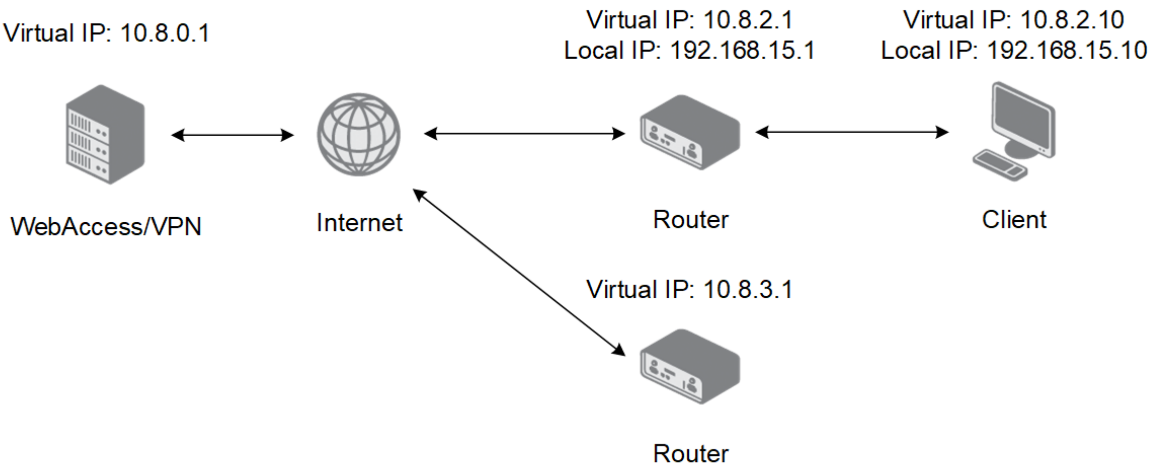


Figure 24: 1:1 NAT Example 1

### 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 subneted 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 device that is located behind eth0 interface and has the address 192.168.15.50. If someone tries to ping 10.8.2.130, it will be delivered to the device that is located behind eth1 interface and has IP address 192.168.15.130.

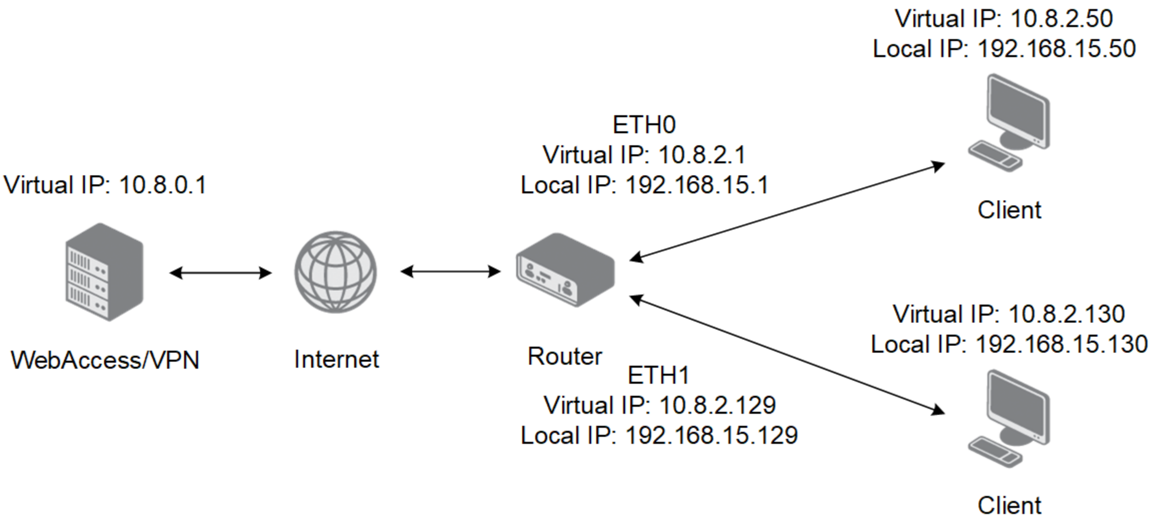


Figure 25: 1:1 NAT Example 2

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 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

Networks can be also divided as in this example, 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.

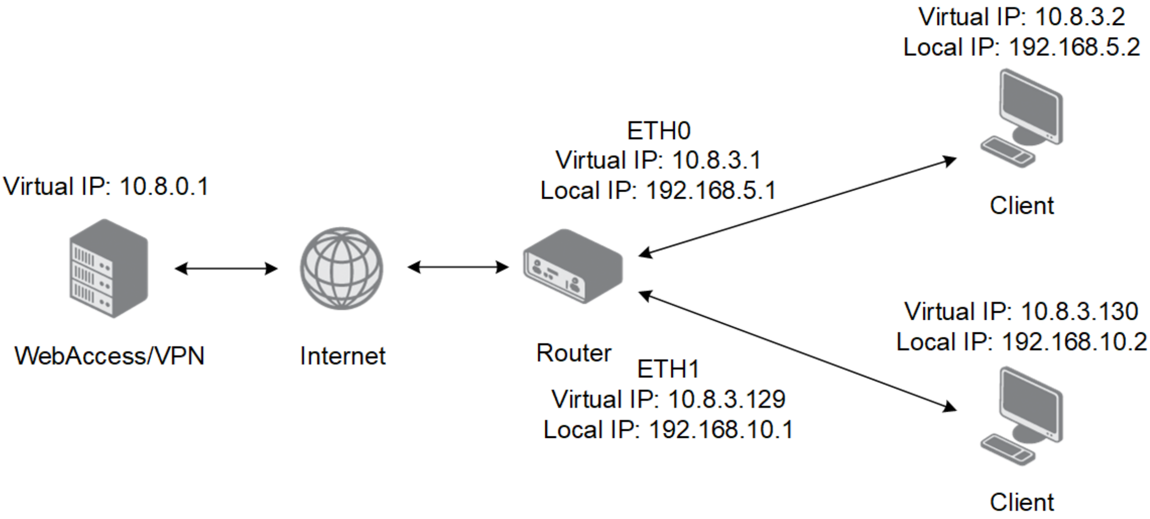


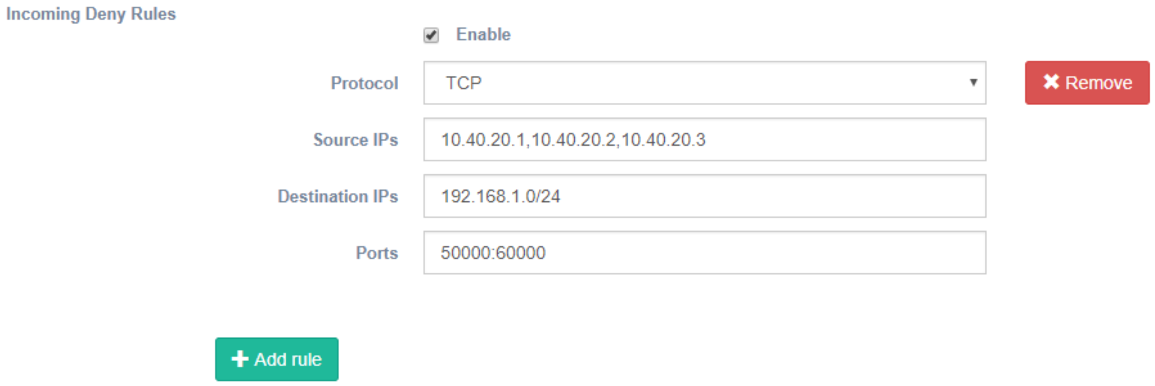
Figure 26: 1:1 NAT Example 3

### 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 router or in one of his LANs.
  - **Outgoing** – applied to packets that come from the router or from 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 you 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 then run it again, 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:



Incoming Deny Rules

☑ Enable

| | |
|---|---|
| Protocol | TCP |
| Source IPs | 10.40.20.1,10.40.20.2,10.40.20.3 |
| Destination IPs | 192.168.1.0/24 |
| Ports | 50000:60000 |

Figure 27: Device Firewall rule example

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

Table 3: Device Firewall rule – options and syntax

### 4.3.4 Routers: Link

Clicking on the *Link* in 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:

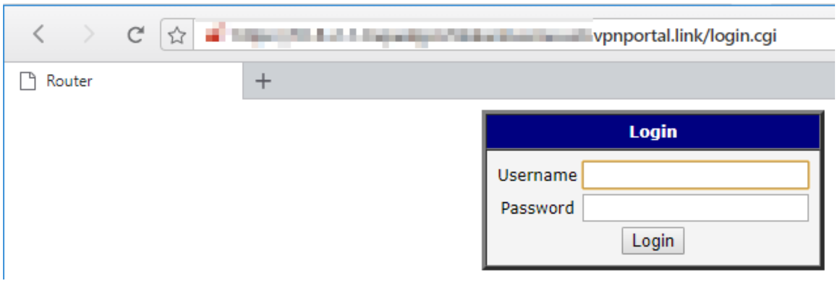


Figure 28: Routers – Link: login to Router via WebAccess/VPN as proxy

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

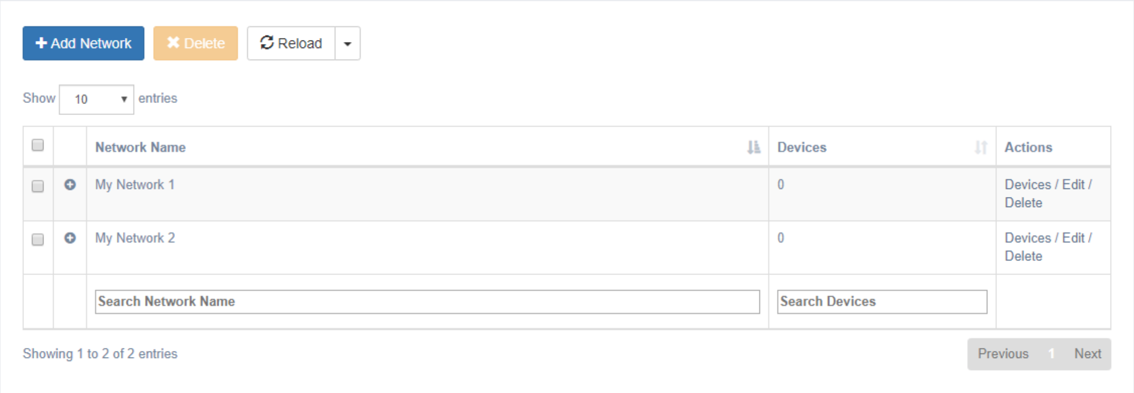
- The DNS records of WebAccess/VPN domain name have to be set, see Chap. 2.2.
- There has to be HTTPS service enabled in the router (*Configuration – Services – HTTP*).
- Proxy has to be enabled for the Router (Router Edit, tab Proxy).

### 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. The Router will lose access to the WebAccess/VPN network. To add the device again in future, the validation process has to be repeated.

## 4.4 Networks

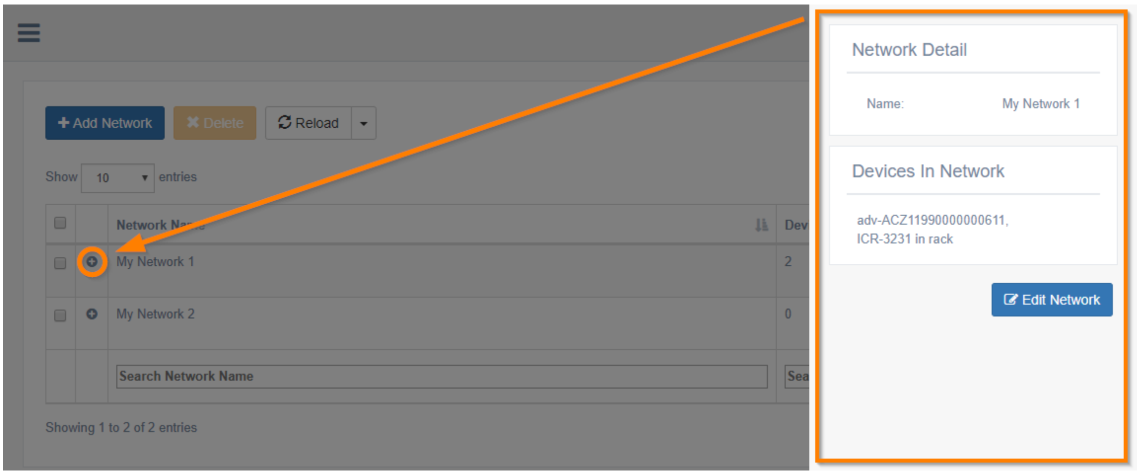
The Routers and Standalone VPN Clients added to WebAccess/VPN can see each other only after they are added into the same Network. Networks can be created or deleted on the *Networks* page, see the Figure below.



| □ | | Network Name | Devices | Actions |
|---|---|---|---|---|
| □ | ⊕ | My Network 1 | 0 | Devices / Edit / Delete |
| □ | ⊕ | My Network 2 | 0 | Devices / Edit / Delete |
| | | Search Network Name | Search Devices | |

Figure 29: Networks in WebAccess/VPN

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



| □ | | Network Name | Dev |
|---|---|---|---|
| □ | ⊕ | My Network 1 | 2 |
| □ | ⊕ | My Network 2 | 0 |
| | | Search Network Name | Sea |

Network Detail

Name: My Network 1

Devices In Network

adv-ACZ11990000000611,
ICR-3231 in rack

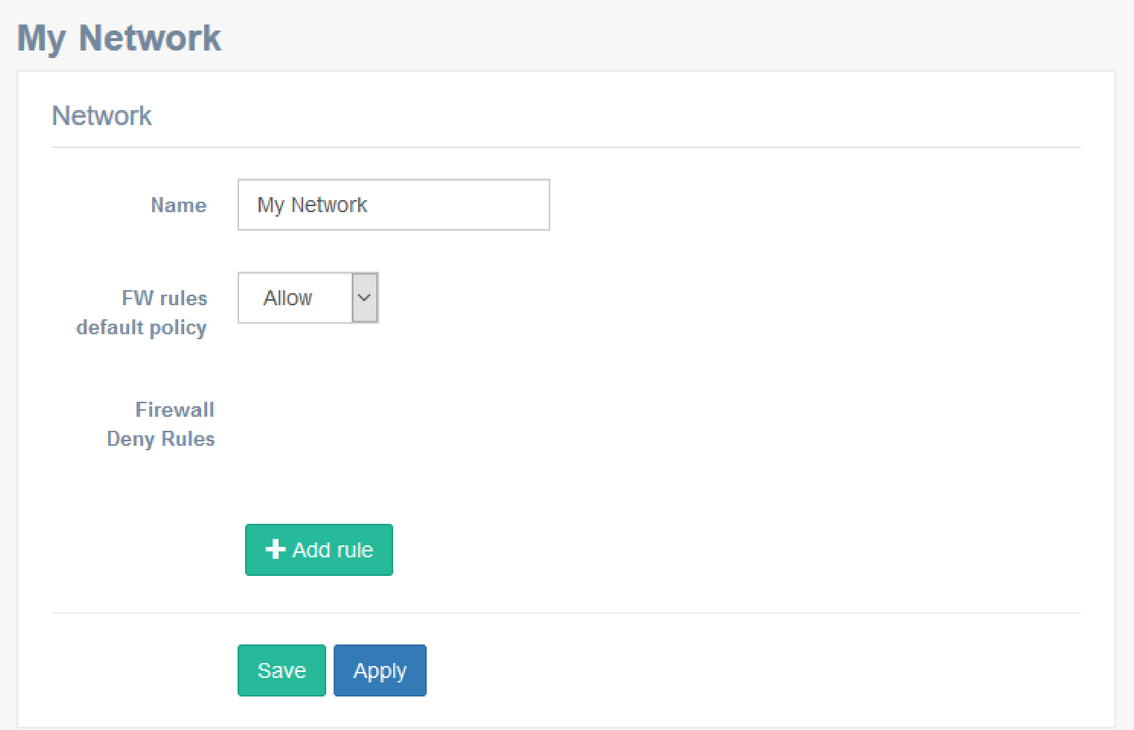
Figure 30: Networks – Network overview

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

- *Detail* – shows the main page of that network, from where you can add/remove its devices. It is the same page as shown 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. Use the green *Add rule* button to create a filtering rule.



My Network

Network

Name: My Network

FW rules default policy: Allow

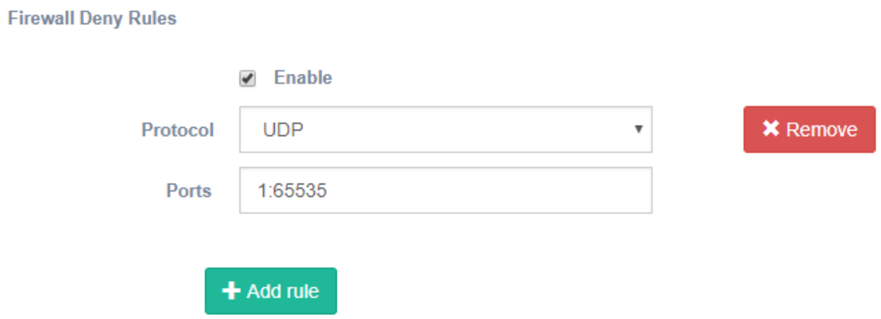
Firewall Deny Rules

Figure 31: Networks – Firewall Rules

- Network firewall rules are only applied to traffic, where both the source and the destination IP addresses belong into the same network.
- Each network has its own default policy and its own 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).



Firewall Deny Rules

☑ Enable

Protocol: UDP

Ports: 1:65535

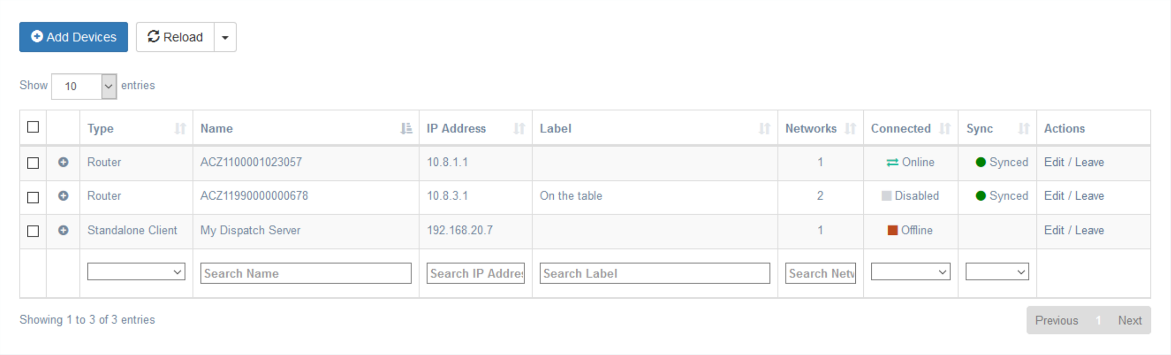
Figure 32: Device Firewall rule example

| 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. Choose the network you want to edit from the dropdown menu on the left.



| ☐ | | Type | Name | IP Address | Label | Networks | Connected | Sync | Actions |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | ⊕ | Router | ACZ1100001023057 | 10.8.1.1 | | 1 | ⇄ Online | ● Synced | Edit / Leave |
| ☐ | ⊕ | Router | ACZ11990000000678 | 10.8.3.1 | On the table | 2 | ▨ Disabled | ● Synced | Edit / Leave |
| ☐ | ⊕ | Standalone Client | My Dispatch Server | 192.168.20.7 | | 1 | 🟥 Offline | | Edit / Leave |
| | | | Search Name | Search IP Addre | Search Label | Search Netw | | | |

Figure 33: Devices in Networks

To add a device into 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.

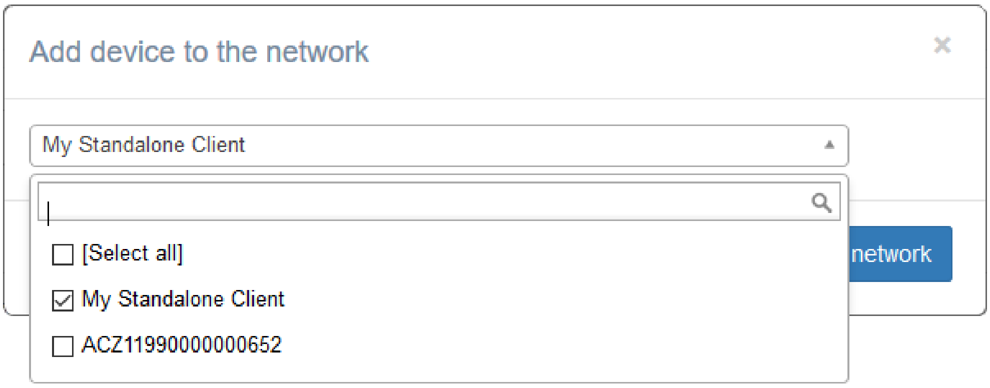


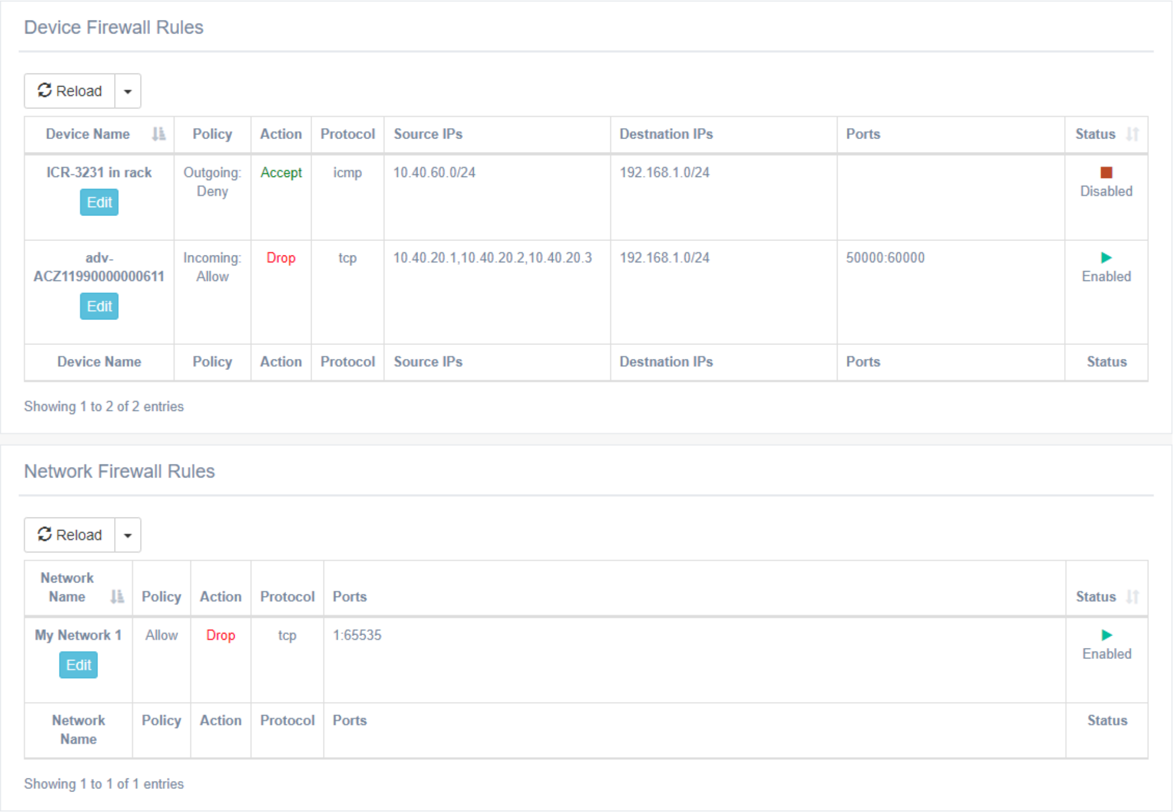
Figure 34: Devices in Networks – add device to network

The columns in the list of Devices in Network are nearly the same as on *Devices* page (there is additional Type column and Sync column is empty for Standalone VPN Clients). You can view details of a device clicking on plus icon next to the *Device Name* as in Figure 15. 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 for networks (section 4.4.1), including their status (enabled/disabled). There are 2 separate types of firewall – Device Firewall and Network Firewall.

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



Device Firewall Rules

| Device Name | Policy | Action | Protocol | Source IPs | Destnation IPs | Ports | Status |
|---|---|---|---|---|---|---|---|
| ICR-3231 in rack<br>Edit | Outgoing: Deny | Accept | icmp | 10.40.60.0/24 | 192.168.1.0/24 | | ■ Disabled |
| adv-ACZ11990000000611<br>Edit | Incoming: Allow | Drop | tcp | 10.40.20.1,10.40.20.2,10.40.20.3 | 192.168.1.0/24 | 50000:60000 | ▶ Enabled |
| Device Name | Policy | Action | Protocol | Source IPs | Destnation IPs | Ports | Status |

Showing 1 to 2 of 2 entries

Network Firewall Rules

| Network Name | Policy | Action | Protocol | Ports | Status |
|---|---|---|---|---|---|
| My Network 1<br>Edit | Allow | Drop | tcp | 1:65535 | ▶ Enabled |
| Network Name | Policy | Action | Protocol | Ports | Status |

Showing 1 to 1 of 1 entries

Figure 35: 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.

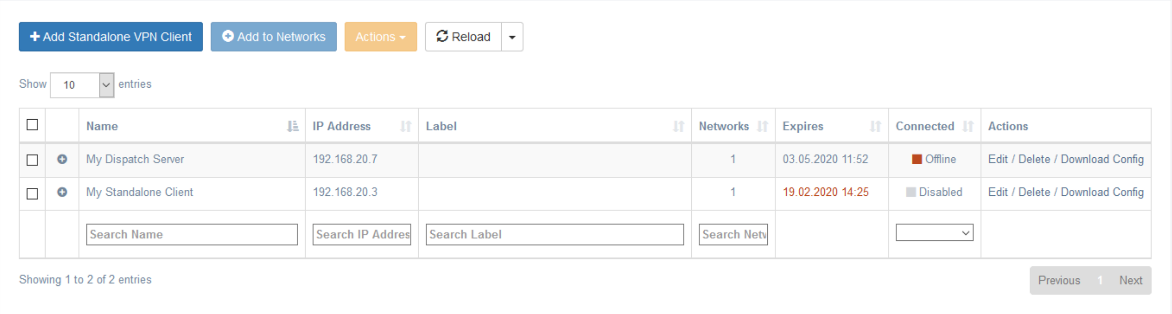
## 4.7 Standalone VPN Clients

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

> Newly added Standalone VPN Client does not see any other Routers or Standalone VPN Clients automatically. 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 Standalone VPN Client the same way as for the Router.

Prerequisities 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 Customer Server.



Show 10 entries

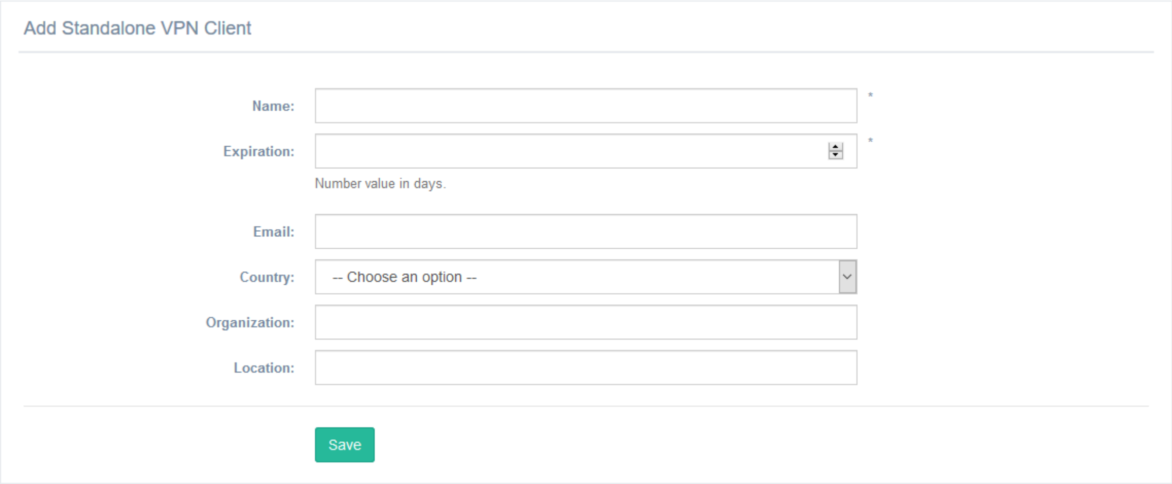
| □ | | Name | IP Address | Label | Networks | Expires | Connected | Actions |
|---|---|---|---|---|---|---|---|---|
| □ | ⊕ | My Dispatch Server | 192.168.20.7 | | 1 | 03.05.2020 11:52 | 🟥 Offline | Edit / Delete / Download Config |
| □ | ⊕ | My Standalone Client | 192.168.20.3 | | 1 | 19.02.2020 14:25 | ▨ Disabled | Edit / Delete / Download Config |
| | | Search Name | Search IP Addres | Search Label | Search Netv | | | |

Showing 1 to 2 of 2 entries

Figure 36: 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 36. Expired clients have red colored date in 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 37. You can set up an expiration of access (in days). The information provided can not be changed later (except for Name) and will be used to create the certificate, private key and configuration file for this Standalone VPN Client.



Add Standalone VPN Client

|  |  |
|---|---|
| Name: | * |
| Expiration: | *<br>Number value in days. |
| Email: |  |
| Country: | -- Choose an option -- |
| Organization: |  |
| Location: |  |

Figure 37: Add a Standalone VPN Client dialogue

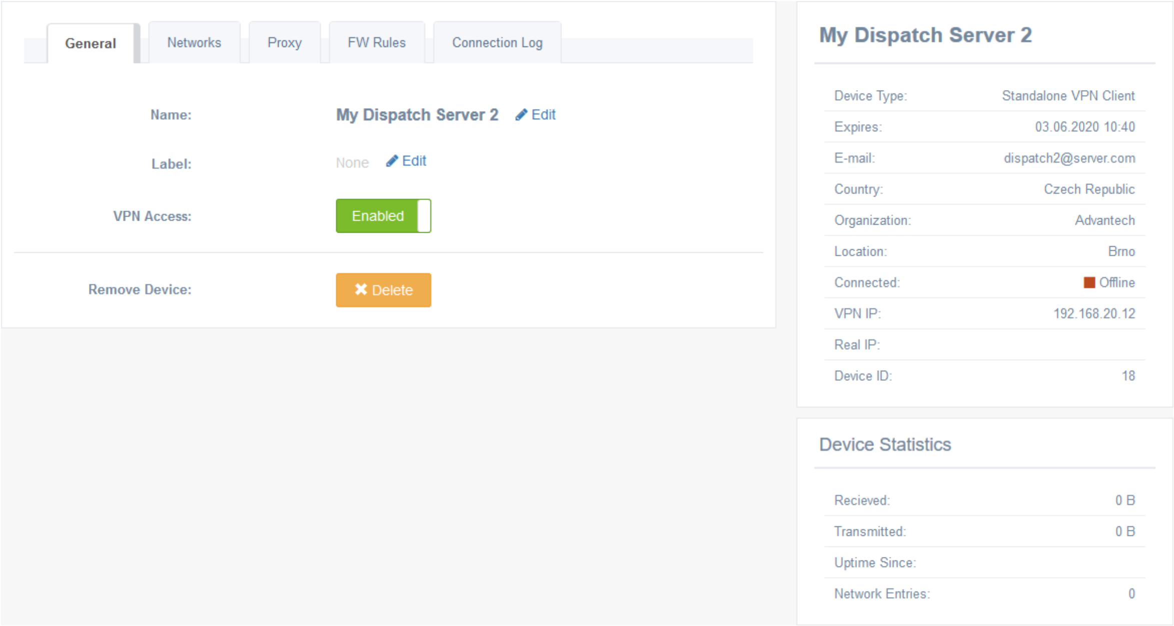
**To connect as Standalone VPN Client:** Download the client configuration file. It is a common OpenVPN configuration file (*.ovpn extension) that contains all keys and certificates needed for an OpenVPN connection. The client configuration files can be downloaded from a list of Standalone VPN Clients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

**To delete a Standalone VPN Client:** Click on *Delete* in 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 Standalone VPN Client using revocated certificate will not be able to connect to WebAccess/VPN any more. **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 Standalone VPN Client as a device similar to Router edit. Expiration date (and other non-required properties) can not be changed.

#### General Tab



Name: My Dispatch Server 2

Label: None

VPN Access: Enabled

Remove Device:

My Dispatch Server 2

| | |
|---|---|
| Device Type: | Standalone VPN Client |
| Expires: | 03.06.2020 10:40 |
| E-mail: | dispatch2@server.com |
| Country: | Czech Republic |
| Organization: | Advantech |
| Location: | Brno |
| Connected: | 🟥 Offline |
| VPN IP: | 192.168.20.12 |
| Real IP: | |
| Device ID: | 18 |

Device Statistics

| | |
|---|---|
| Recieved: | 0 B |
| Transmitted: | 0 B |
| Uptime Since: | |
| Network Entries: | 0 |

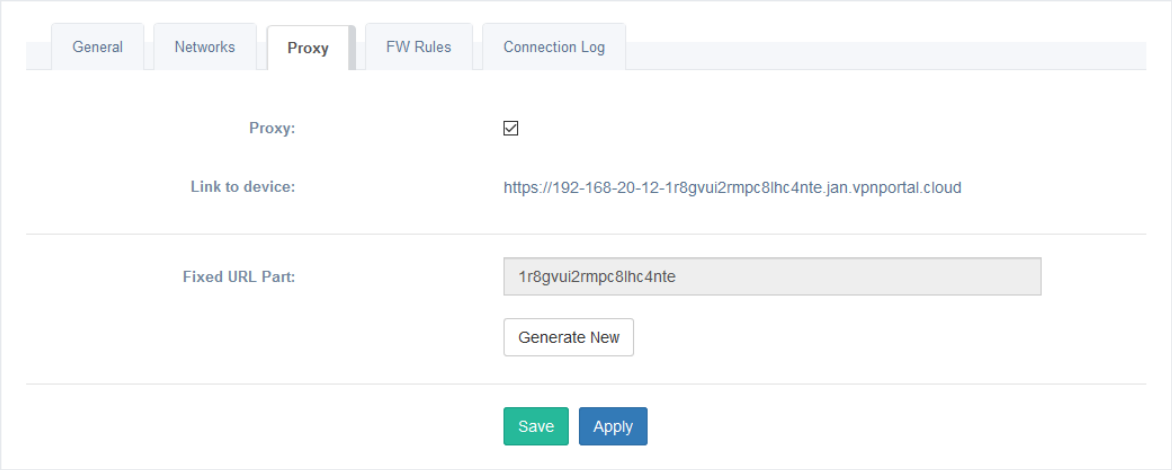
Figure 38: Edit Standalone VPN Client – General

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



Proxy: ☑

Link to device: https://192-168-20-12-1r8gvui2rmpc8lhc4nte.jan.vpnportal.cloud

Fixed URL Part: 1r8gvui2rmpc8lhc4nte

Figure 39: Edit Standalone VPN Client – Proxy

Enable or disable the proxy for Standalone VPN Client. Same as described in 4.3.1, except for LAN Proxy is not available. 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 server, intranet server, etc. Not so for traveller's Android phone or laptop. The default state is affected by Proxy settings in *Administration – Settings*.

### FW Rules Tab

Firewall rules 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

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

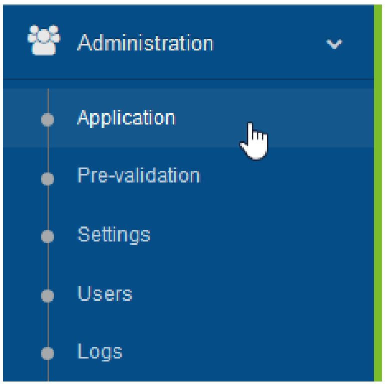
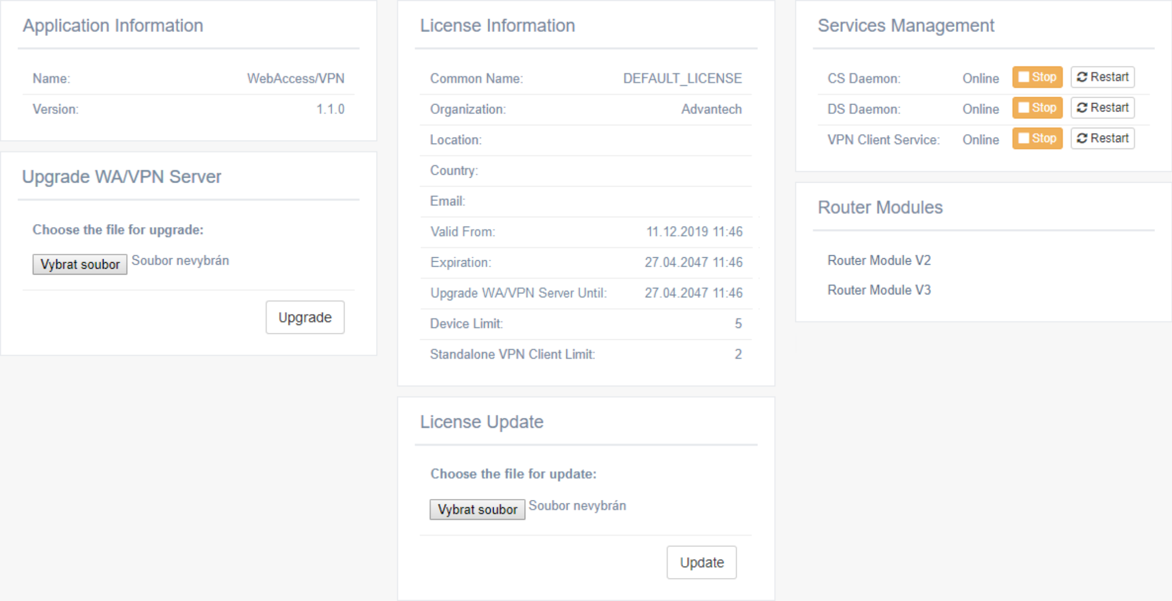


Figure 40: Administration submenu

### 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. Show here is application information and actions that may be taken, see further sections.



Application Information

| | |
|---|---|
| Name: | WebAccess/VPN |
| Version: | 1.1.0 |

Upgrade WA/VPN Server

Choose the file for upgrade:

Vybrat soubor Soubor nevybrán

Upgrade

License Information

| | |
|---|---|
| Common Name: | DEFAULT_LICENSE |
| Organization: | Advantech |
| Location: | |
| Country: | |
| Email: | |
| Valid From: | 11.12.2019 11:46 |
| Expiration: | 27.04.2047 11:46 |
| Upgrade WA/VPN Server Until: | 27.04.2047 11:46 |
| Device Limit: | 5 |
| Standalone VPN Client Limit: | 2 |

License Update

Choose the file for update:

Vybrat soubor Soubor nevybrán

Update

Services Management

| | | | |
|---|---|---|---|
| CS Daemon: | Online | Stop | Restart |
| DS Daemon: | Online | Stop | Restart |
| VPN Client Service: | Online | Stop | Restart |

Router Modules

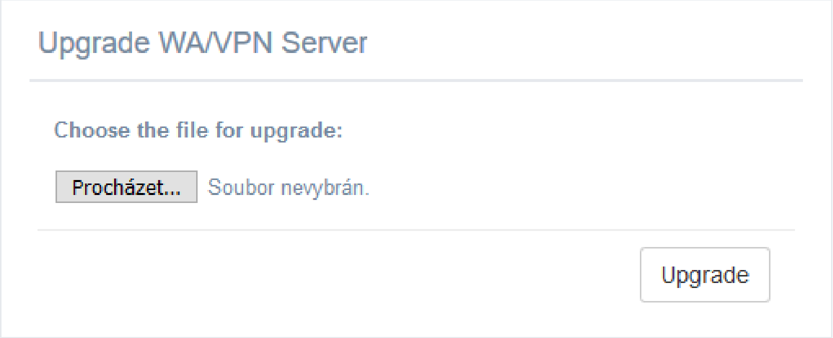
Router Module V2

Router Module V3

Figure 41: Application Management

### Upgrade WebAccess/VPN Server

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



Upgrade WA/VPN Server

Choose the file for upgrade:

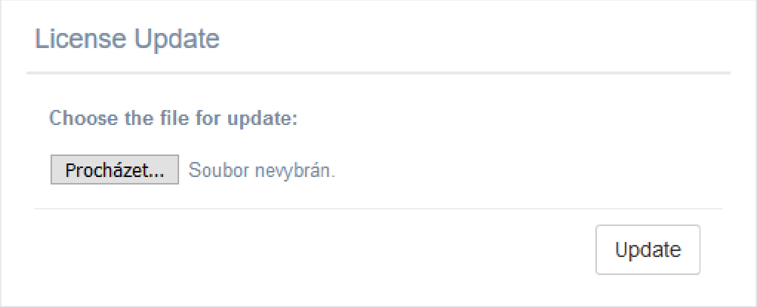
Figure 42: Upgrade WebAccess/VPN Server

! Allow the WebAccess/VPN a few minutes to upgrade. Do not refresh the browser during 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 be also 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 to update the license file. Choose the .tar.gz license file and click the *Update* button.



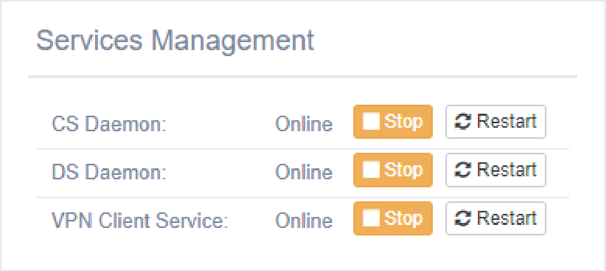
License Update

Choose the file for update:

Figure 43: 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 form 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 useful for troubleshooting – it is possible to check whether services are running.



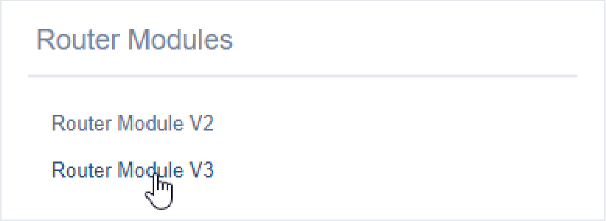
Services Management

| | | | |
|---|---|---|---|
| CS Daemon: | Online | □ Stop | ⟳ Restart |
| DS Daemon: | Online | □ Stop | ⟳ Restart |
| VPN Client Service: | Online | □ Stop | ⟳ Restart |

Figure 44: WebAccess/VPN services management

### Download User Modules

You can easily download user modules for your Advantech routers to add them to WebAccess/VPN.



Router Modules

Router Module V2

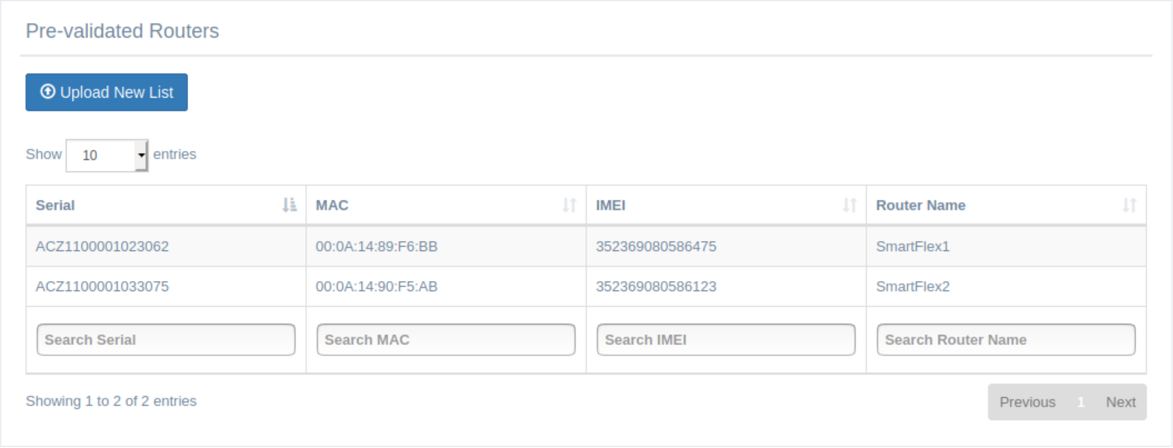
Router Module V3

Figure 45: Download user modules 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 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.



Pre-validated Routers

| Serial | MAC | IMEI | Router Name |
|---|---|---|---|
| ACZ1100001023062 | 00:0A:14:89:F6:BB | 352369080586475 | SmartFlex1 |
| ACZ1100001033075 | 00:0A:14:90:F5:AB | 352369080586123 | SmartFlex2 |

Showing 1 to 2 of 2 entries

Figure 46: Logs

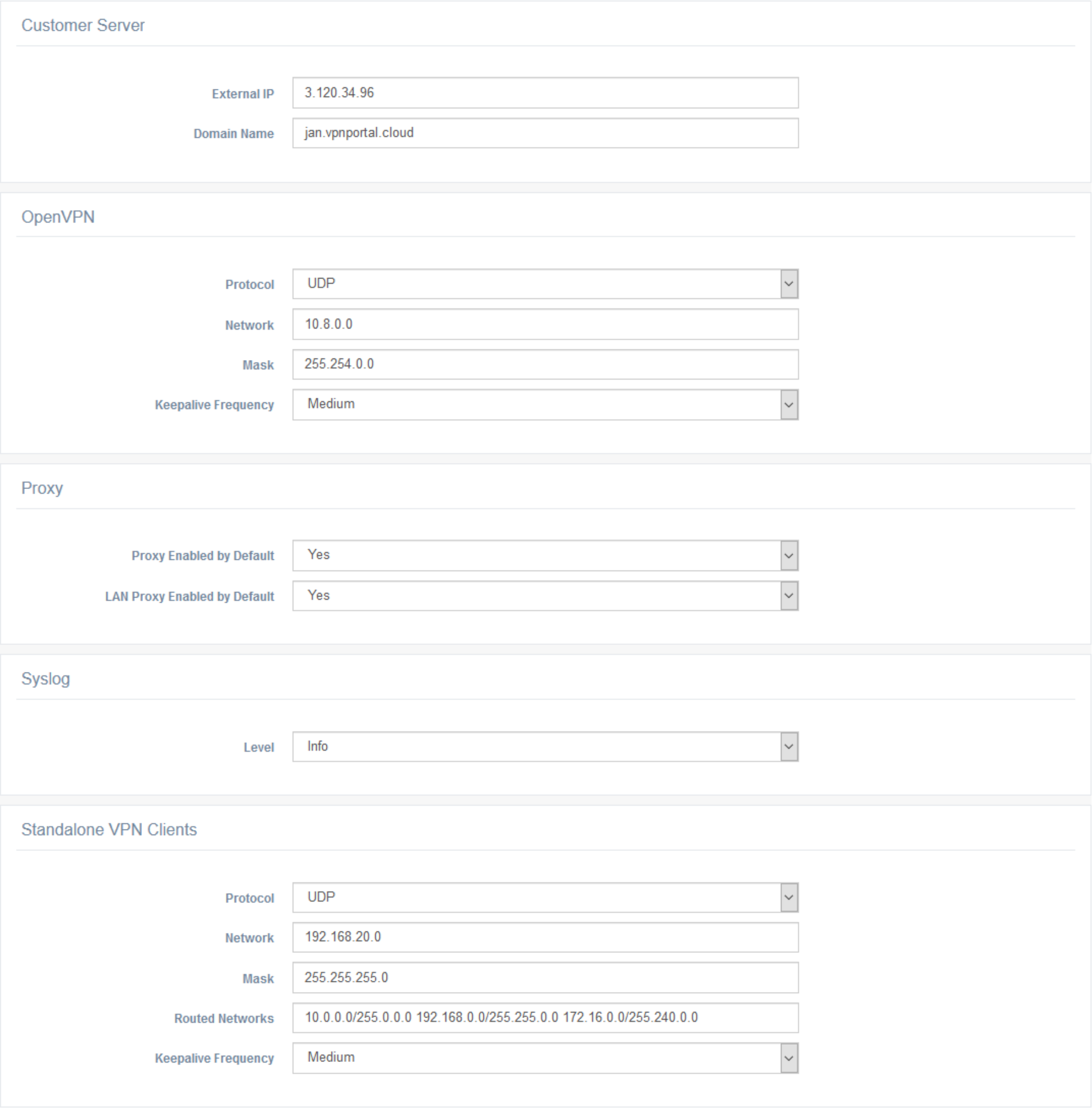
The format of the list file has to be TXT file with the following structure. Note that the number of commas has to remain the same on all lines. Sharp character can be used as a comment.

```
# 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 items explained in the table below.



Customer Server

| | |
|---|---|
| External IP | 3.120.34.96 |
| Domain Name | jan.vpnportal.cloud |

OpenVPN

| | |
|---|---|
| Protocol | UDP |
| Network | 10.8.0.0 |
| Mask | 255.254.0.0 |
| Keepalive Frequency | Medium |

Proxy

| | |
|---|---|
| Proxy Enabled by Default | Yes |
| LAN Proxy Enabled by Default | Yes |

Syslog

| | |
|---|---|
| Level | Info |

Standalone VPN Clients

| | |
|---|---|
| Protocol | UDP |
| Network | 192.168.20.0 |
| Mask | 255.255.255.0 |
| Routed Networks | 10.0.0.0/255.0.0.0 192.168.0.0/255.255.0.0 172.16.0.0/255.240.0.0 |
| Keepalive Frequency | Medium |

Figure 47: Settings of WebAccess/VPN

| Setting | Description |
|---|---|
| **Customer Server** | |
| External IP | The IP address of CS that will be given to routers. 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 newly added device. Can be managed additionaly in device Edit. |
| LAN Proxy Enabled by Default | The default state of LAN Proxy for newly added Router. Can be managed additionaly in Router Edit. |
| **OpenVPN** | |
| Protocol | The OpenVPN Tunnel with Routers is established via UDP (default) or TCP, based on this setting. Useful for cases when UDP is blocked by firewall. **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<br>Mask | 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 that are used to check connection state of individual devices. 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 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 |
| **Standalone VPN Clients** | |
| Protocol | The OpenVPN Tunnel with Standalone VPN Clients is established via UDP (default) or TCP, based on this setting. **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. |

Continued on next page

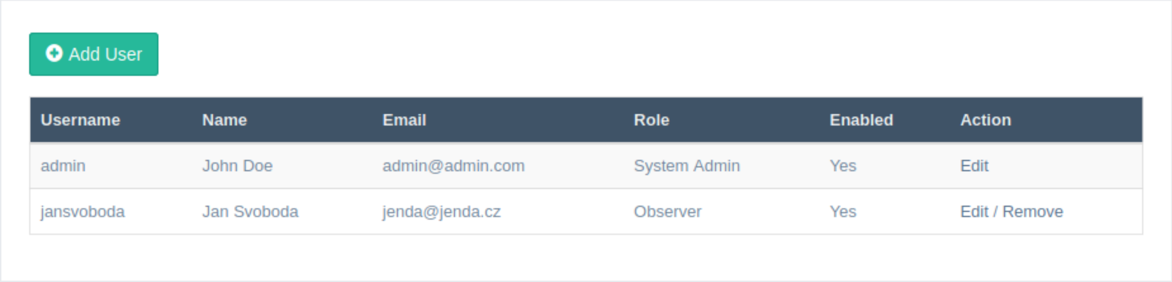
Continued from previous page

| Device Property | Description |
|---|---|
| Network<br>Mask | 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 that are used to check connection state of individual devices. 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 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.



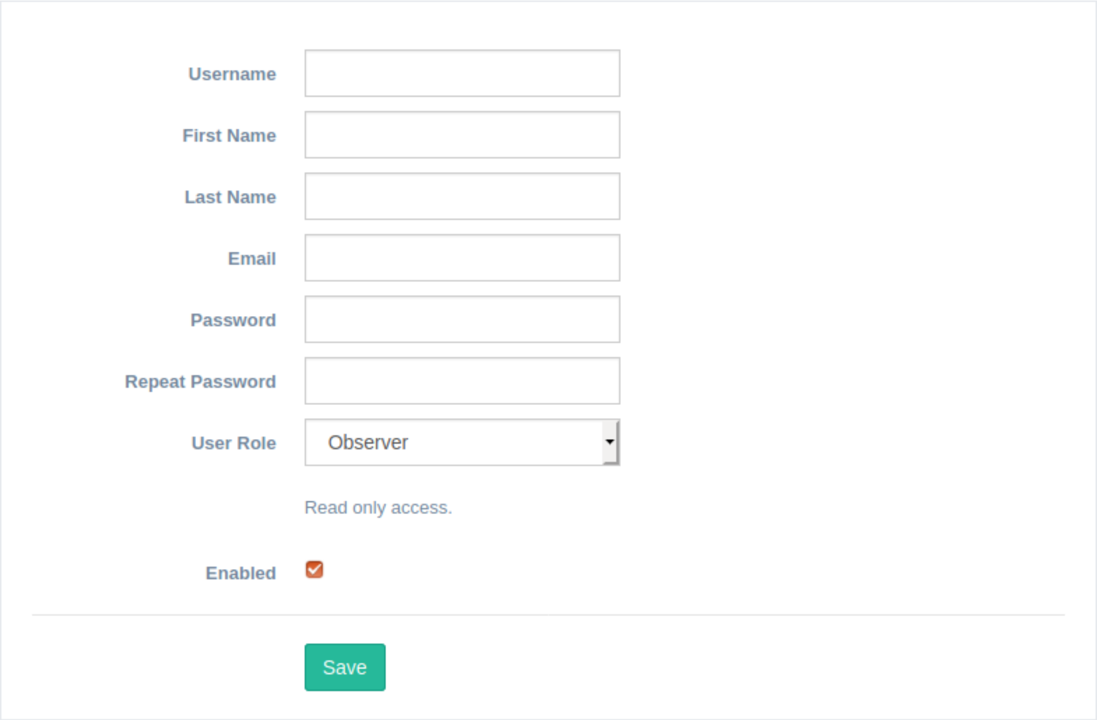
⊕ Add User

| Username | Name | Email | Role | Enabled | Action |
|---|---|---|---|---|---|
| admin | John Doe | admin@admin.com | System Admin | Yes | Edit |
| jansvoboda | Jan Svoboda | jenda@jenda.cz | Observer | Yes | Edit / Remove |

Figure 48: 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 user is stored in WebAccess/VPN and the account can be enabled again in future (by the user with System Admin role).



| | |
|---|---|
| Username | |
| First Name | |
| Last Name | |
| Email | |
| Password | |
| Repeat Password | |
| User Role | Observer |
| | Read only access. |
| Enabled | ☑ |

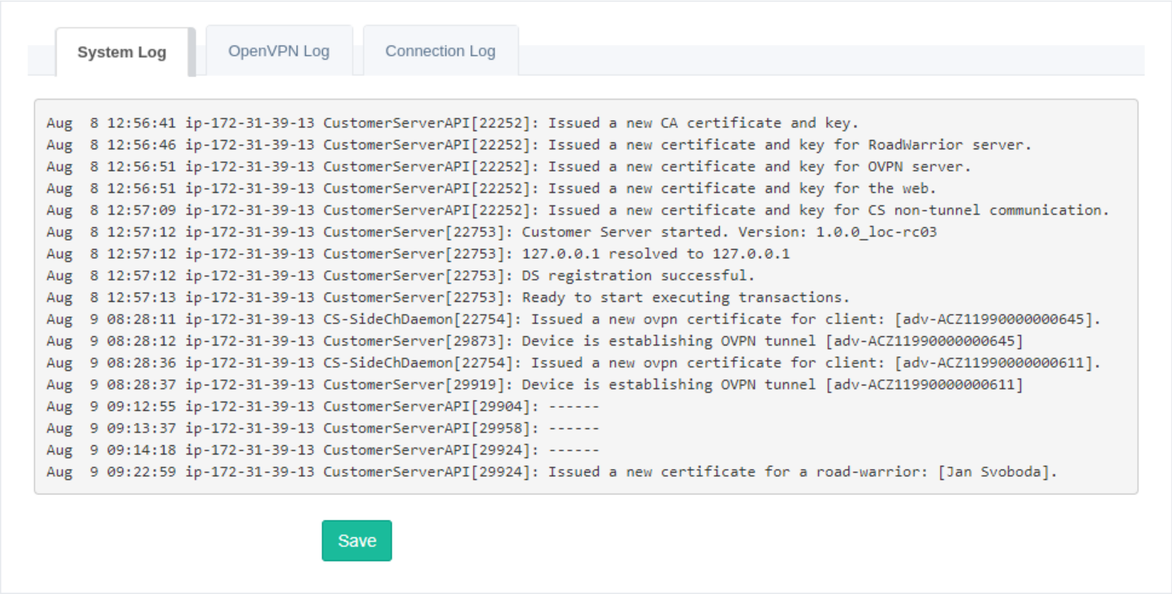
Figure 49: User Edit

Roles are defined as follows. The definition is hierarchical – it means that 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 device to/from 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), can change settings and administer 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.



```
Aug  8 12:56:41 ip-172-31-39-13 CustomerServerAPI[22252]: Issued a new CA certificate and key.
Aug  8 12:56:46 ip-172-31-39-13 CustomerServerAPI[22252]: Issued a new certificate and key for RoadWarrior server.
Aug  8 12:56:51 ip-172-31-39-13 CustomerServerAPI[22252]: Issued a new certificate and key for OVPN server.
Aug  8 12:56:51 ip-172-31-39-13 CustomerServerAPI[22252]: Issued a new certificate and key for the web.
Aug  8 12:57:09 ip-172-31-39-13 CustomerServerAPI[22252]: Issued a new certificate and key for CS non-tunnel communication.
Aug  8 12:57:12 ip-172-31-39-13 CustomerServer[22753]: Customer Server started. Version: 1.0.0_loc-rc03
Aug  8 12:57:12 ip-172-31-39-13 CustomerServer[22753]: 127.0.0.1 resolved to 127.0.0.1
Aug  8 12:57:12 ip-172-31-39-13 CustomerServer[22753]: DS registration successful.
Aug  8 12:57:13 ip-172-31-39-13 CustomerServer[22753]: Ready to start executing transactions.
Aug  9 08:28:11 ip-172-31-39-13 CS-SideChDaemon[22754]: Issued a new ovpn certificate for client: [adv-ACZ11990000000645].
Aug  9 08:28:12 ip-172-31-39-13 CustomerServer[29873]: Device is establishing OVPN tunnel [adv-ACZ11990000000645]
Aug  9 08:28:36 ip-172-31-39-13 CS-SideChDaemon[22754]: Issued a new ovpn certificate for client: [adv-ACZ11990000000611].
Aug  9 08:28:37 ip-172-31-39-13 CustomerServer[29919]: Device is establishing OVPN tunnel [adv-ACZ11990000000611]
Aug  9 09:12:55 ip-172-31-39-13 CustomerServerAPI[29904]: ------
Aug  9 09:13:37 ip-172-31-39-13 CustomerServerAPI[29958]: ------
Aug  9 09:14:18 ip-172-31-39-13 CustomerServerAPI[29924]: ------
Aug  9 09:22:59 ip-172-31-39-13 CustomerServerAPI[29924]: Issued a new certificate for a road-warrior: [Jan Svoboda].
```

Figure 50: 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.

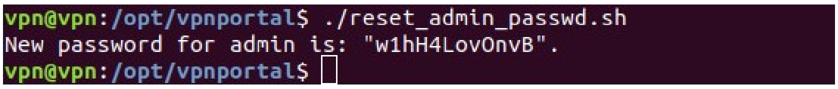
# 5. Advanced Management

## 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 following commands:

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

As a response, the new generated password will be printed to 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 user module's *VPN Portal* web page:
*OpenVPN Tunnel* – shows the status of the OpenVPN tunnel.
*WebAccess/VPN* – shows the status of the user module.

### 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),
available from: https://ep.advantech-bb.cz

**[2]** Advantech Czech: **SmartStart Configuration Manual** (MAN-0022-EN),
available from: https://ep.advantech-bb.cz

**[3]** Advantech Czech: **SmartFlex Configuration Manual** (MAN-0023-EN),
available from: https://ep.advantech-bb.cz

**[4]** Advantech Czech: **SmartMotion Configuration Manual** (MAN-0024-EN),
available from: https://ep.advantech-bb.cz

**[5]** Engineering Portal: **https://ep.advantech-bb.cz/**

# A. Standalone Hardware Test

**Test Description:** A single Network was created in WebAccess/VPN. All the devices were added to this Network. Then, randomly 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 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 →**<br>**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 1: 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 was 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 "top" program. |

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