

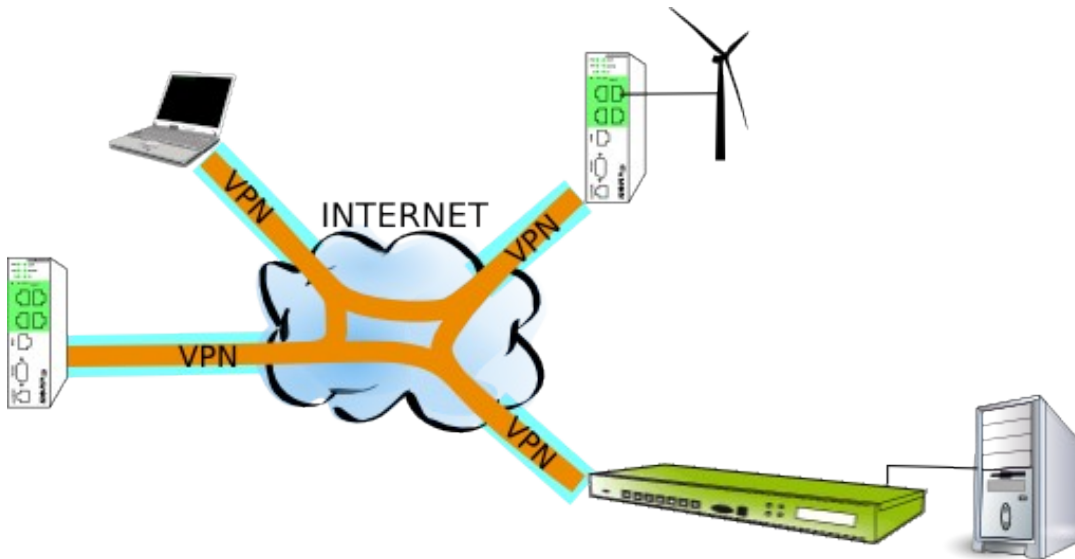
eWON Application User Guide

AUG 021 / Rev 1.0



You Select, We Connect

ENDIAN with eWON Getting started



Content

This guide will explain in a few steps how to configure and use your ENDIAN to create a VPN network with eWONs.

1. Hardware and software requirements.....	3
Hardware requirements.....	3
Software requirements.....	3
eWON Firmware Version.....	3
2. What is ENDIAN for eWON?.....	4
What is ENDIAN?.....	4
What is ENDIAN for eWON?.....	4
3. Network Setup.....	5
ENDIAN configuration.....	5
ENDIAN Connection.....	5
Interfaces Configuration.....	6
OpenVPN Configuration.....	9
eWON Configuration.....	13
PC configuration.....	15
4. Network topologies.....	17
Only eWONs.....	17
ENDIAN Settings.....	17
Only eWONs + eWONs see eWONs.....	18
ENDIANSettings.....	18
eWONs + Local network of eWONs + eWONs see eWONs.....	19
ENDIAN Settings.....	19
5. Security.....	21
Revisions.....	23

Hardware and software requirements

Hardware requirements

In order to follow this guide you'll need:

- 1 ENDIAN server appliance (in this document, we use an ENDIAN-Mini)
- 1 (or several) eWON-VPN with an Internet access

Software requirements

eWON configuration software:

The eWON is configured through its web server. So all you need is a standard Web Browser software like Internet Explorerⁱ or Firefoxⁱⁱ.

Additionally we suggest you to download the eBuddy utility on our website :
<http://support.ewon.biz>.

This utility allows to list all the eWONs on your network and to change the default IP address of an eWON to match your LAN IP address range. With eBuddy you can also easily upgrade the firmware of your eWON (if required).

eWON Firmware Version

To be able to follow this guide your eWON needs a firmware version 5.5 or higher. A simple way to do an eWON firmware upgrade is to use eBuddy, the eWON software companion.

What is ENDIAN for eWON?

What is ENDIAN?

ENDIAN is an *Open Source Firewall UTM Appliance*.

Website: <http://www.endian.com>

The Endian Firewall is an open source Linux distribution that specializes on Routing/Firewalling and Unified Threat Management. It is being developed by the Italian Endian Srl and the community.

The version of the Endian Firewall used in this document is version 2.2.1.

ENDIAN is mainly a Firewall (both directions), but also a **"Virtual Private Network (VPN) Gateway with OpenVPN or IPsec"**.

Other features are: *DHCP-Server, Hotspot/Wireless Security, Web Antivirus, Web Antispam, E-Mail Antivirus, E-Mail Antispam, Transparent HTTP-Proxy, Content Filter, SIP VoIP Support, Network Address Translation, Multi IP address (aliases), HTTPS web interface, Connection statistics, Log of networking traffic, Forwarding of logs to an external server, NTP-Server, Intrusion Detection System, ADSL-Modem Support*

What is ENDIAN for eWON?

As eWON-VPN are based on OpenVPN too, it is easy to build a VPN network with an ENDIAN as OpenVPN Server and eWONs as OpenVPN Clients.

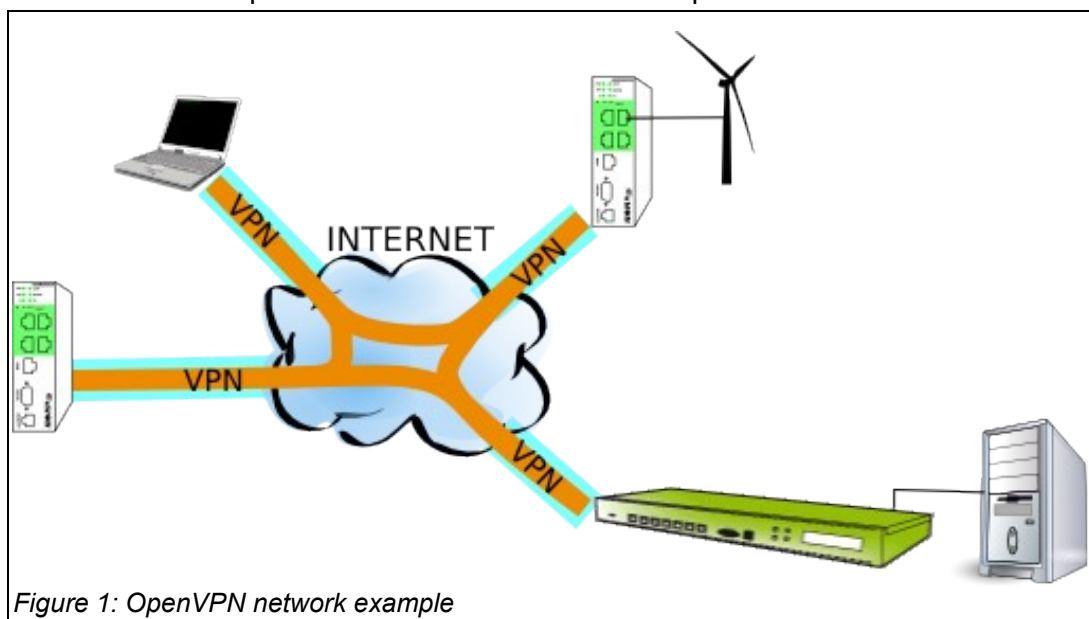


Figure 1: OpenVPN network example

Network Setup

ENDIAN configuration

ENDIAN Connection

By default, you can access the ENDIAN appliance by its LAN Ethernet connector.

The default IP LAN address range is the 192.168.0.0/24 and the ENDIAN Firewall is at 192.168.0.15.

The system will redirect you to the <https://192.168.0.15:10443> and you will accept the Certificate to login into the ENDIAN.

Then, a popup will invite you to enter the Login/Password of the ENDIAN.

Default login: *admin*
 Default pwd: *endian*

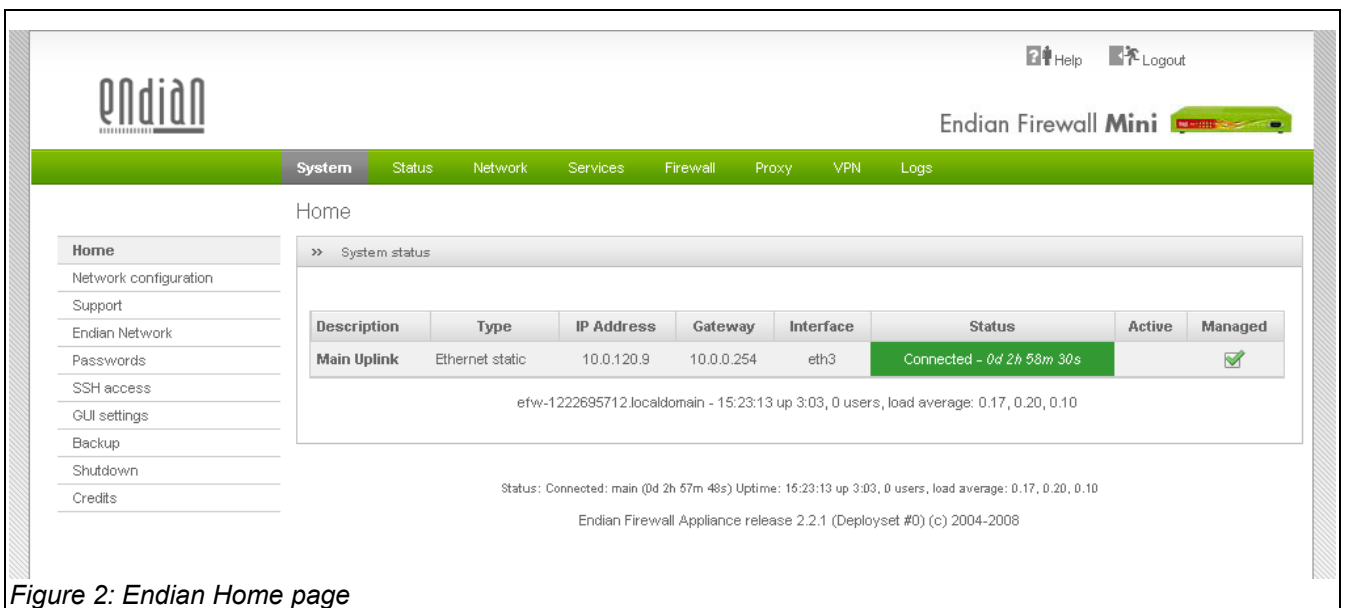
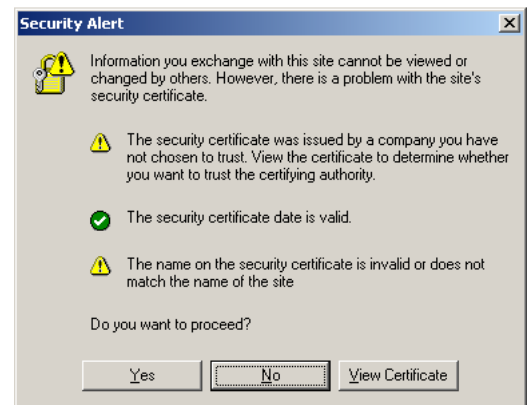


Figure 2: Endian Home page

Interfaces Configuration

ENDIANs are built to manage 4 hardware interfaces. In this document, we only need 2 hardware interfaces to build our VPN network.

In our simple VPN network, we need only a LAN and a WAN interfaces.

LAN: our private network

LAN address range 192.168.0.0/24

ENDIAN-LAN: 192.168.0.15

WAN: the corporate network allowing us to access Internet

WAN address range 10.0.0.0/16

ENDIAN-WAN: 10.0.120.9

Use the *Network configuration* menu and follow the wizard to define and configure the network interfaces.

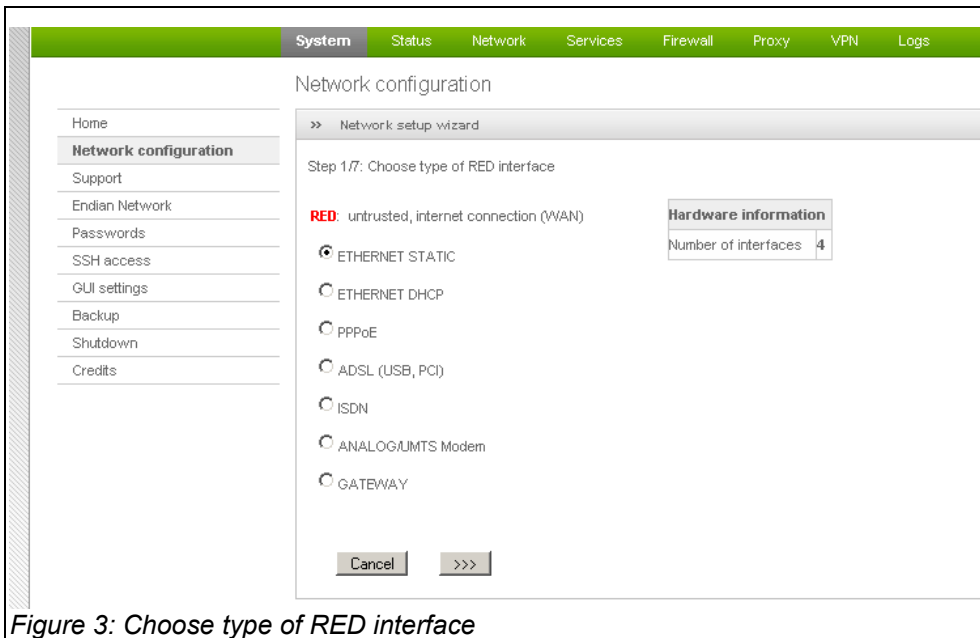


Figure 3: Choose type of RED interface

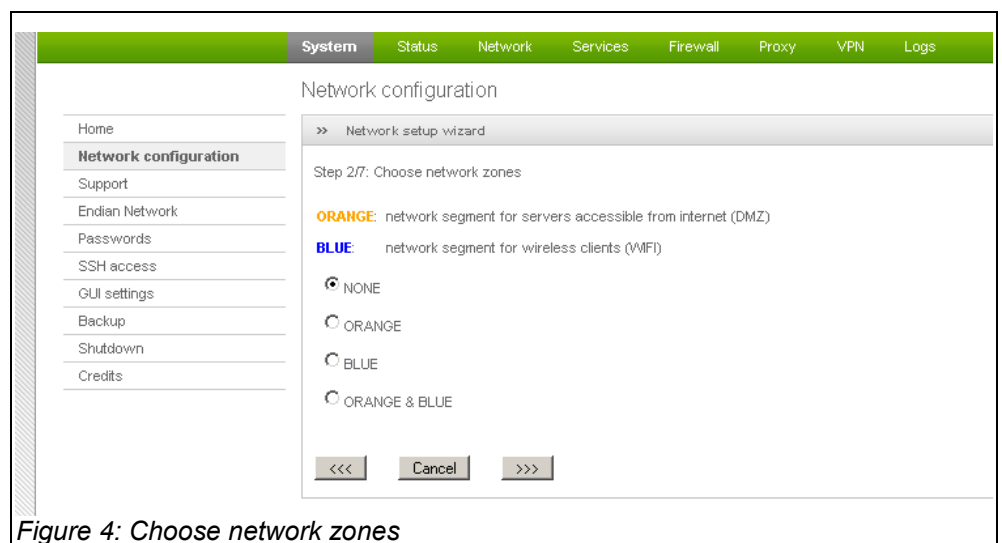


Figure 4: Choose network zones

3. Network Setup

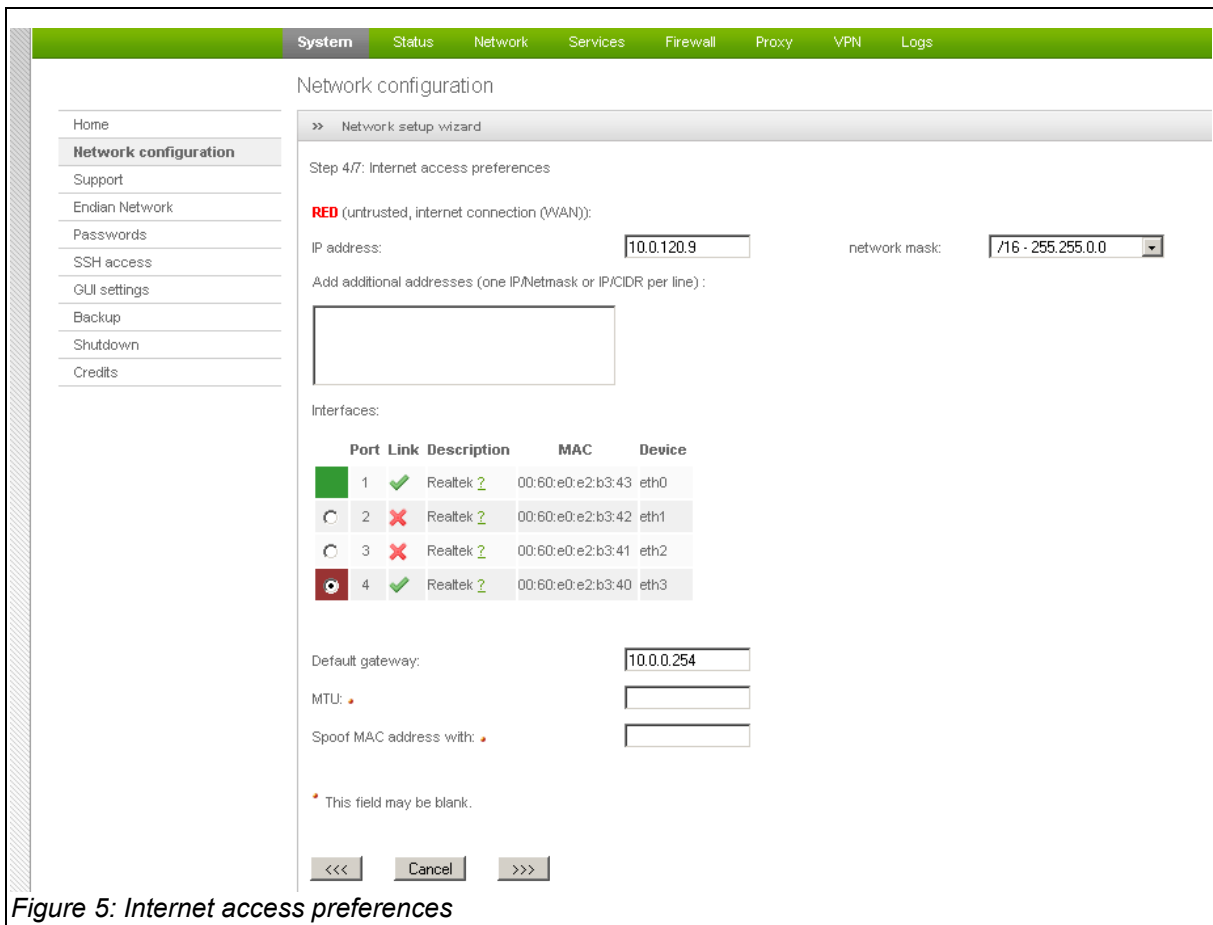


Figure 5: Internet access preferences

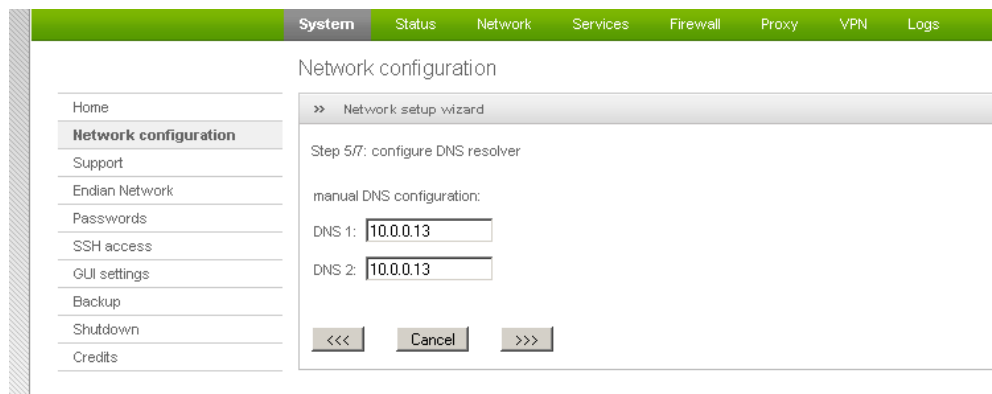


Figure 6: Configure DNS resolver

3. Network Setup

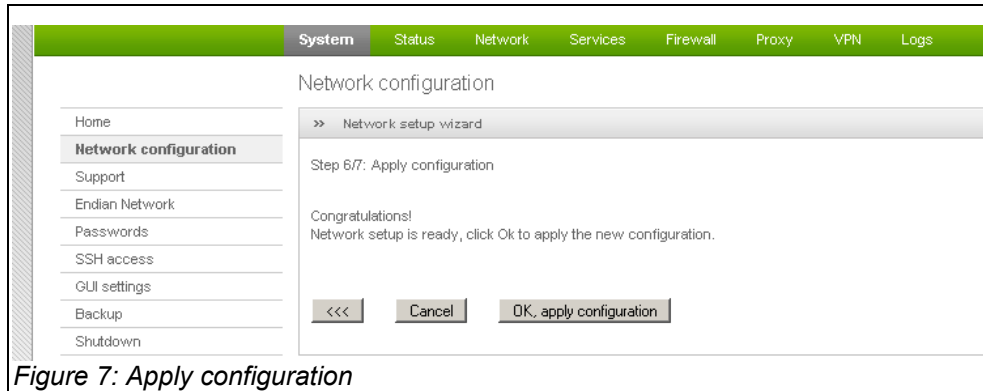


Figure 7: Apply configuration

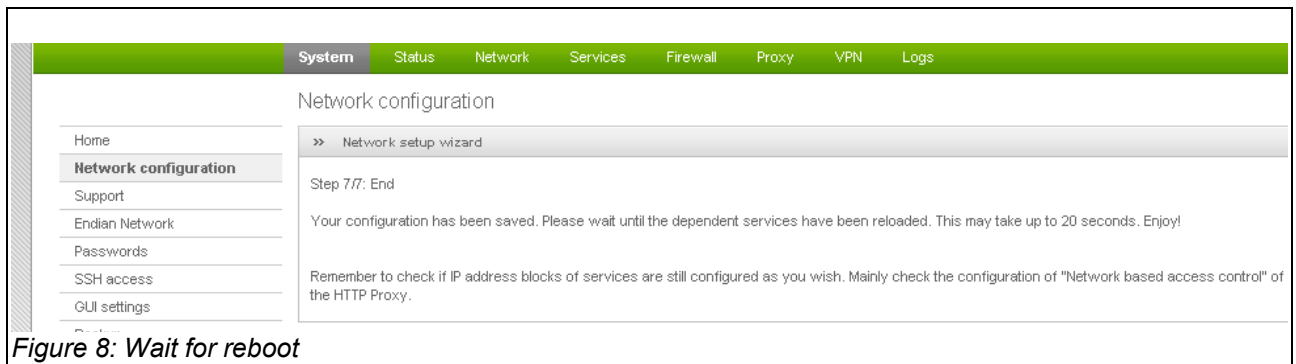


Figure 8: Wait for reboot

OpenVPN Configuration

Global settings

To configure the VPN of the ENDIAN, use the *VPN* top menu, followed by the *OpenVPN server* in the left menu.

The only thing to do is to enable the OpenVPN server and to fix the Dynamic IP pool addresses used by VPN Clients.

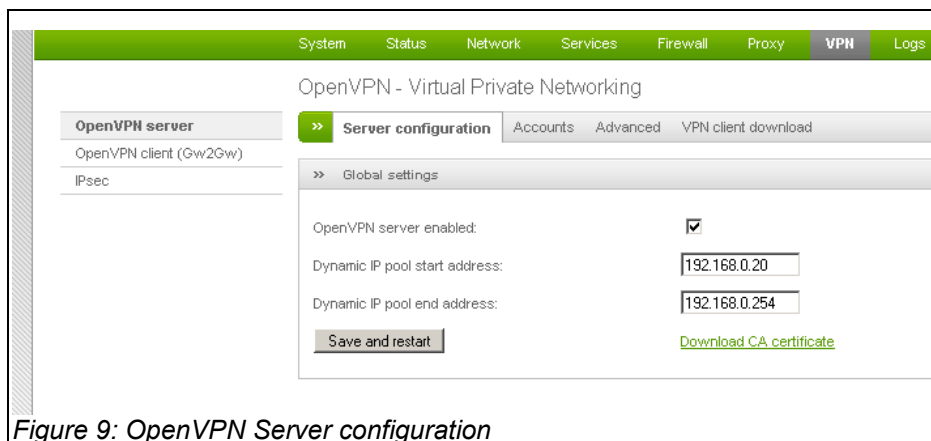


Figure 9: OpenVPN Server configuration

One practical feature of ENDIAN VPN is that all VPN-Clients will receive a VPN address compatible with the LAN network.

In our example, as the LAN (our GREEN interface) is 192.168.0.0/24, all the VPN clients will receive an address between 192.168.0.20 and 192.168.0.254.

NOTE Then, from any devices placed on the LAN, all the remote eWONs connected by VPN will be reachable the same way as if they were physically on the same LAN!



Accounts

Now, for each client, you need to create an account. For that, select the *Accounts* tab and use the *Add Account* button.

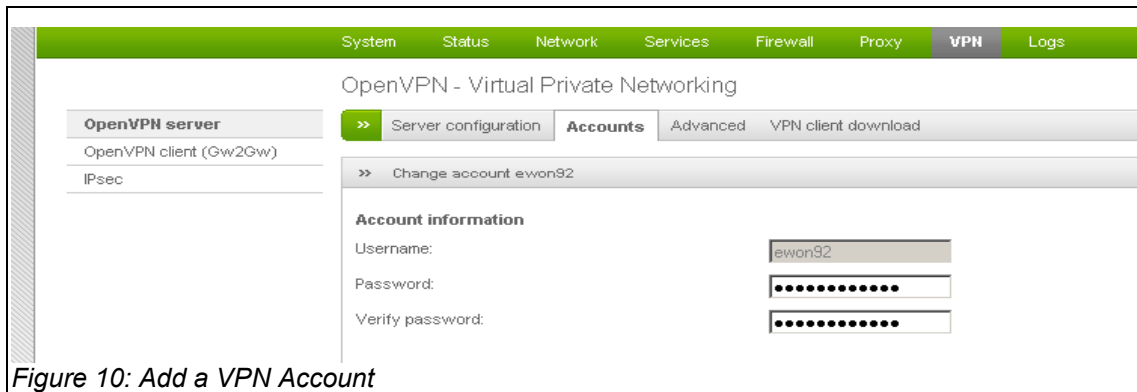


Figure 10: Add a VPN Account

For now, just enter the *Username* and *Password* and save your account. Leave all the other parameters blank, we will discuss them later.

Create as much accounts as you need.

Advanced parameters

With the *Advanced* tab, you will set the *Port* and *Protocol* used for the VPN (UDP 1194 by default) and select the Authentication type (PSK).

Check the *Block DHCP responses coming from tunnel* parameter to avoid DHCP traffic between DHCP-Servers from different places.

Uncheck the *Don't block traffic between clients* to block communication between VPN Clients.

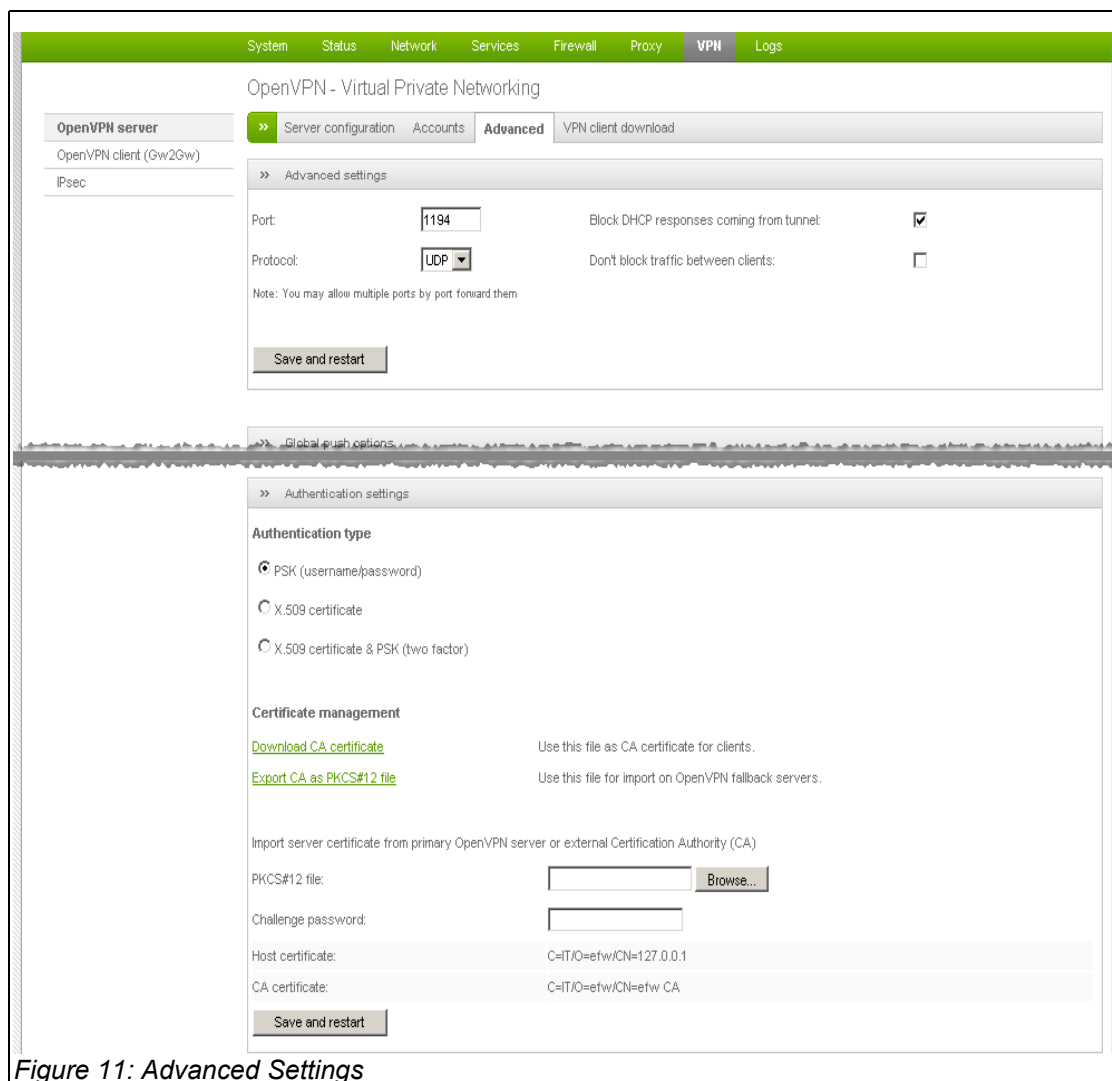


Figure 11: Advanced Settings

Use the *Download CA certificate* link to retrieve the certificate of the Firewall. You will need it to configure your eWONs.

IMPORTANT

Verify that the Port and Protocol used (i.e.: UDP 1194) reaches the ENDIAN firewall.

- Verify that the UDP 1194 packets are not blocked by the ISP (usually, on domestic ADSL offer, incoming traffic is firewalled).
 - Verify that the corporate router forwards all UDP 1194 packets to the ENDIAN.
-

eWON Configuration

Firstly, configure your eWON to access the Internet.

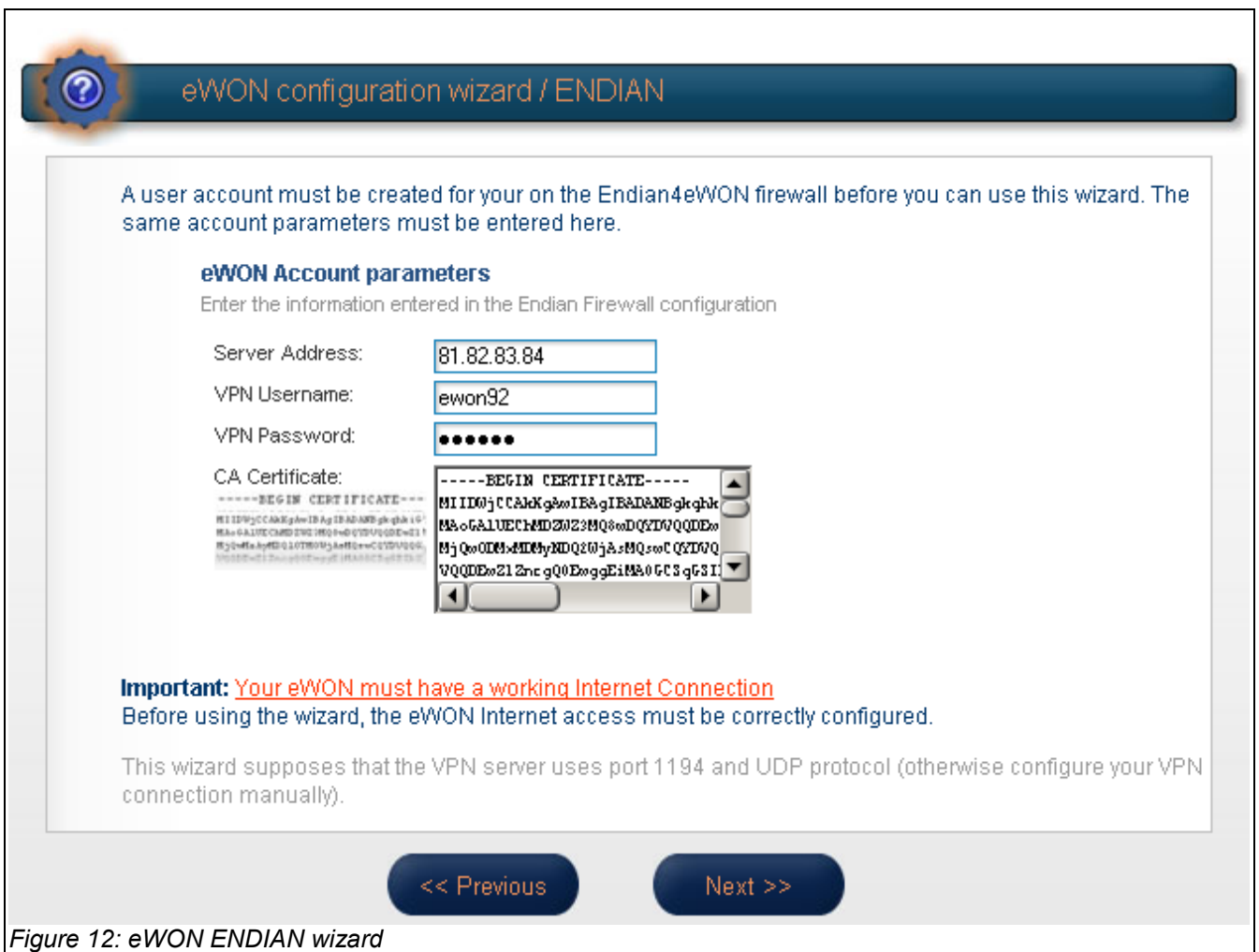
And then, go to the Wizard menu.



Choose the "Configure Endian For eWON connectivity" button



Set the parameters for the ENDIAN connection.



The VPN Username/Password comes from one of the Accounts created in the ENDIAN.

Copy the Certificate downloaded from the ENDIAN.

The Server Address is usually the Internet Public IP address behind which the ENDIAN is placed.

Click on the *Next* button and the eWON will do the VPN connection.

3. Network Setup

If the connection succeeds, you will have the following screen.

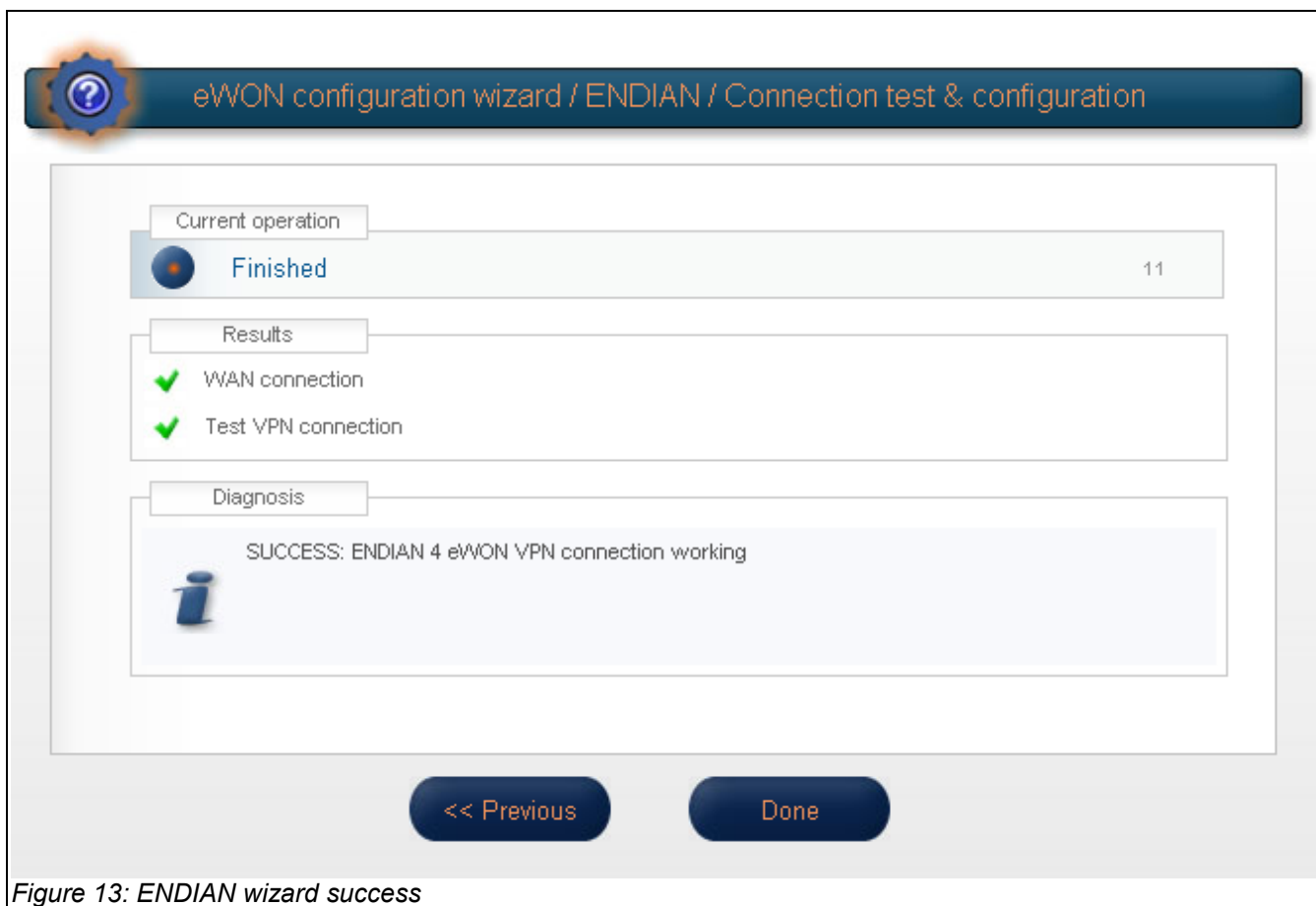


Figure 13: ENDIAN wizard success

If you look at the ENDIAN website, you can view that the eWON92 is well connected.

System Status Network Services Firewall Proxy **VPN** Logs

OpenVPN - Virtual Private Networking

OpenVPN server
OpenVPN client (Gw2Gw)
IPsec

>> **Server configuration** Accounts Advanced VPN client download

>> Global settings

OpenVPN server enabled:

Dynamic IP pool start address:

Dynamic IP pool end address:


[Save and restart](#) [Download CA certificate](#)

>> Connection status and control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions
ewon92	192.168.0.25	10.0.120.92	1.6 KiB / 10 KiB	Thu Dec 4 15:31:13 2008	< 1m	kill ban
prk	192.168.0.24	10.0.120.1	46.6 KiB / 33.5 KiB	Thu Dec 4 15:30:36 2008	1m	kill ban

PC configuration

The ENDIAN Servers are mainly designed to build the PC's network. To connect a PC to your VPN network, you need to install a piece of software on your computer.

From the ENDIAN website, download and install the  EndianVPNClient-setup software.

Once installed, you have your *ENDIAN VPN Dialer* to connect your PC to the OpenVPN network.



Figure 14: ENDIAN VPN Dialer

To join a VPN Network, create or edit a *Profile*.

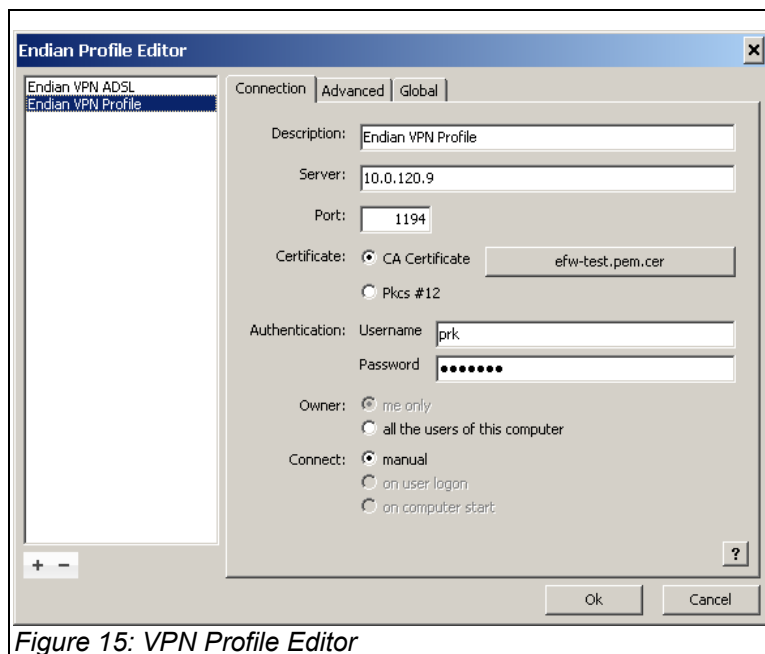


Figure 15: VPN Profile Editor

You need the same certificate as the one used to configure the eWON.

3. Network Setup

Once connected, your PC has access to the whole corporate network (connected to the ENDIAN LAN interface).



Figure 16: PC VPN Client connected

Network topologies

Only eWONs

Now, with the simple configuration of ENDIAN and eWONs done in the previous chapter (only with default settings), we have build a network like the one below:

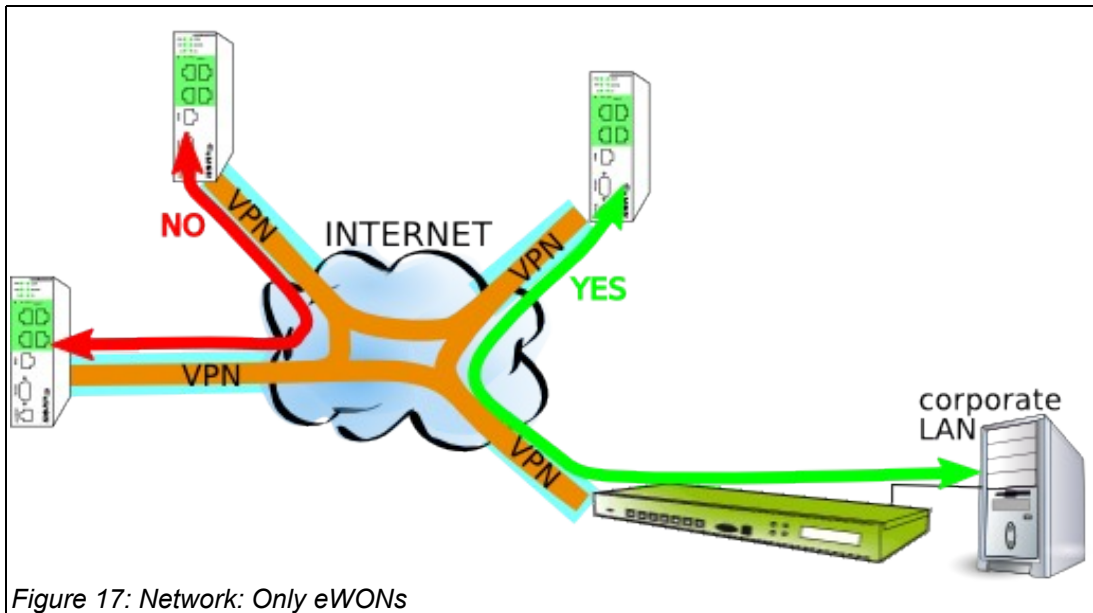
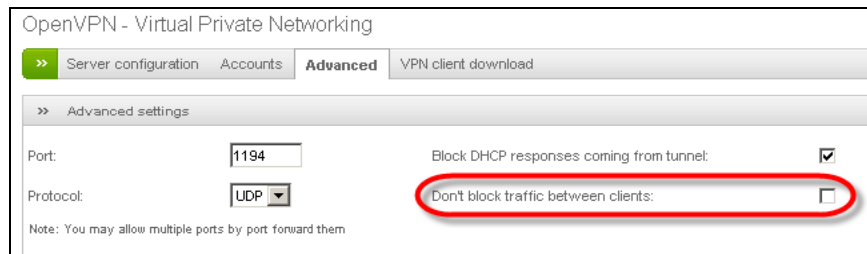


Figure 17: Network: Only eWONs

With this topology:

- All the devices on the corporate LAN have access to all the eWONs
- All the eWONs have access to all the devices on the corporate LAN
- none of the eWONs have access to other eWONs

ENDIAN Settings



Only eWONs + eWONs see eWONs

You can configure the ENDIAN firewall to allow each eWON (VPN Clients) to see all the others.

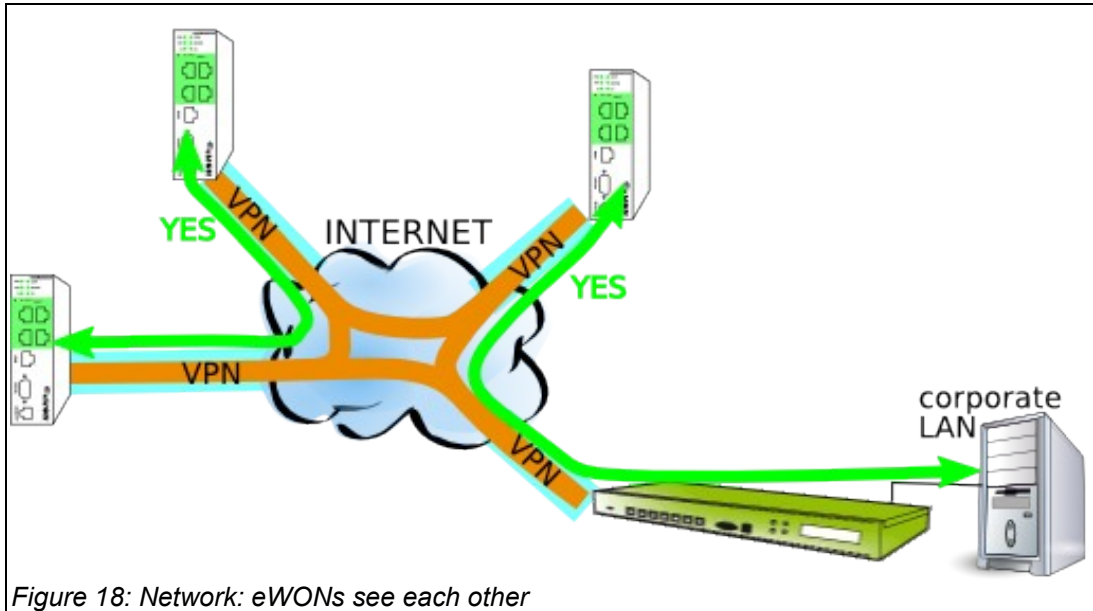


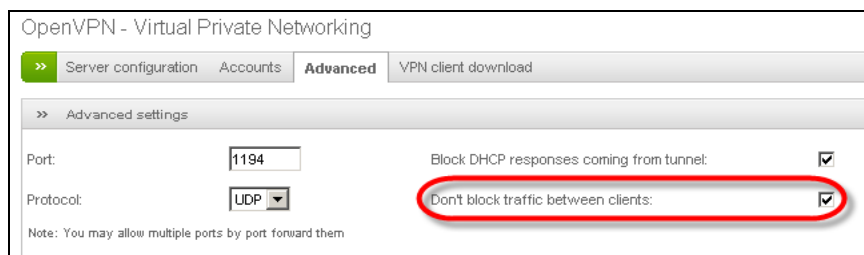
Figure 18: Network: eWONs see each other

With this topology:

- All the devices on the corporate LAN have access to all the eWONs
- All the eWONs have access to all the devices on the corporate LAN
- All the eWONs have access to other eWONs

ENDIAN Settings

To achieve this Global VPN inter-Clients communication, you need to allow it in the *Advanced* settings of the ENDIAN VPN Server.



eWONs + Local network of eWONs + eWONs see eWONs

If you have a local network behind the eWONs, you can configure the ENDIAN Server to automatically handle the routes to these networks.

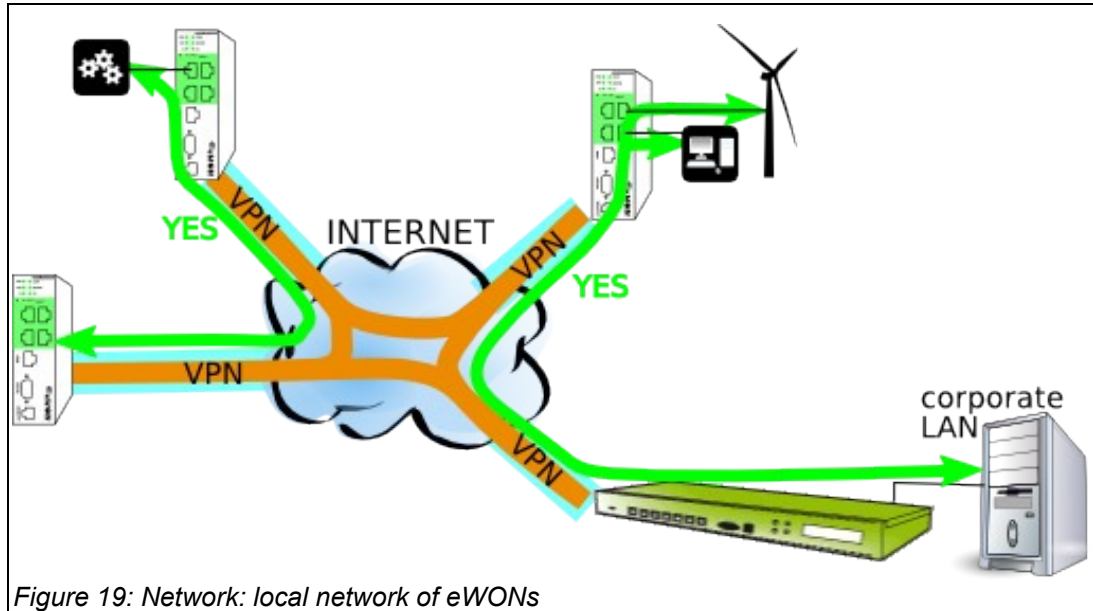


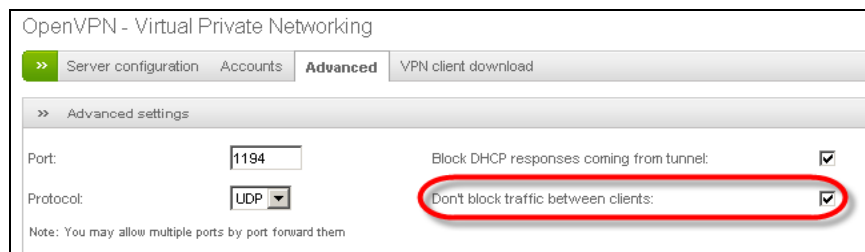
Figure 19: Network: local network of eWONs

With this topology:

- All the devices on the corporate LAN have access to all the eWONs and to devices behind these eWONs
- All the devices on the corporate LAN have access to all the devices behind eWONs
- All the eWONs have access to all the devices on the corporate LAN
- All the devices behind the eWONs have access to all the devices on the corporate LAN
- All the eWONs and devices behind have access to other eWONs and devices behind

ENDIAN Settings

In Advanced settings, allow traffic between clients.



And in each Accounts, you need to set the *Networks behind client*.

The screenshot shows the 'Accounts' configuration page for OpenVPN. The 'Networks behind client' field is highlighted with a red circle and contains the value '10.1.110.0/24'. Other fields include 'Username' (ewon92), 'Password', 'Verify password', 'Direct all client traffic through the VPN server' (checkbox), 'Don't push any routes to client' (checkbox), 'Push only these networks', 'Static ip addresses', 'Push these nameservers', and 'Push domain'. A 'Save' button is at the bottom.

Figure 20: Account settings: with network

IMPORTANT



After changing the networks settings, the ENDIAN Server will invite you to restart the OpenVPN server.

This restart will disconnect all the VPN Clients (and they will automatically reconnect to the OpenVPN).

This OpenVPN reboot is required because when you change an account, maybe you have changed one of the Client Routing settings, and then the ENDIAN Server must send to all the VPN clients these new parameters.

Security

The previous chapter "Network topologies" allows you to globally design the shape of your network. For example, if you want the eWON_1 to have access to the corporate LAN and to one other eWON only, you cannot achieve that with the ENDIAN VPN configuration only.

To allow you to accurately define who has access to who in your VPN network, you need to use the Firewall functionality of the ENDIAN Server and more specifically the VPN Firewall.



Figure 21: VPN Firewall disabled

By default, this VPN Firewall is disabled. To enable it click on the switch button.

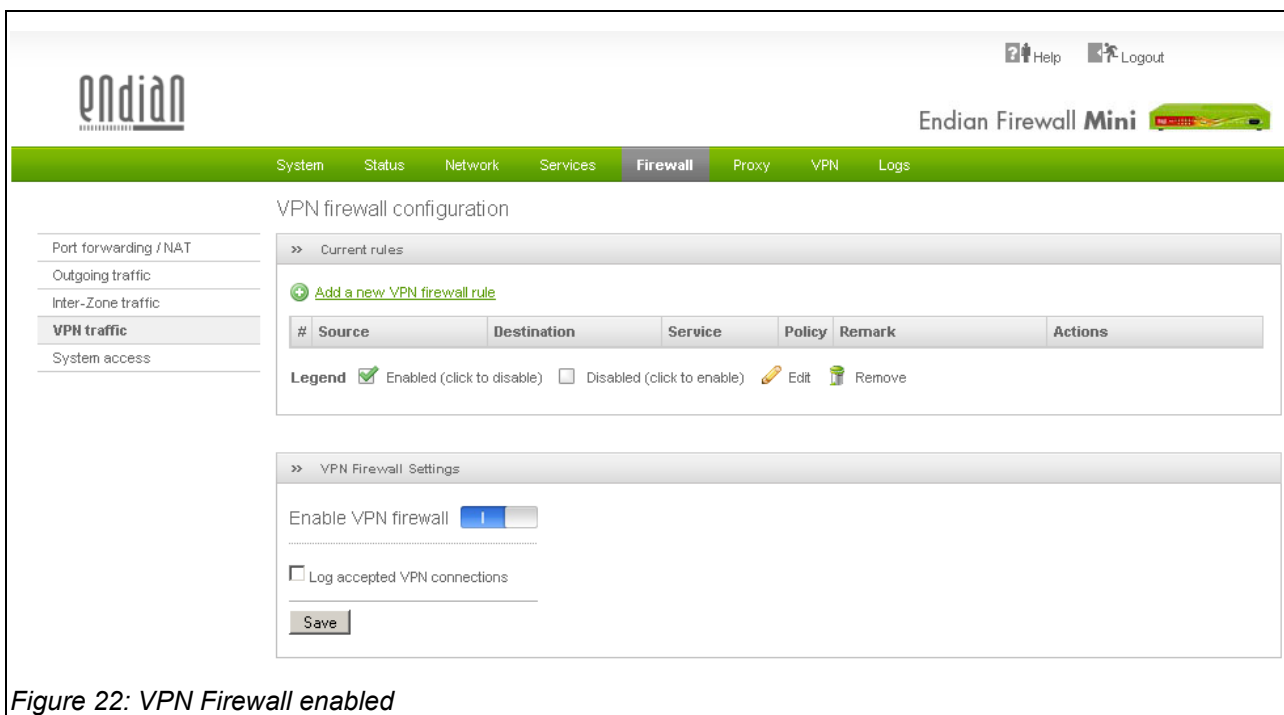


Figure 22: VPN Firewall enabled

5. Security

Now, the VPN Firewall is enabled and blocks all the VPN traffic because there is no rules defined. Click on the [+ Add a new VPN firewall rule](#) link to create a rule.

Then, if you want to allow one user to access all the other VPN Clients, select the Source Type *User* and choose the name of the User in the list.

In Destination, select the type *User* and choose *<ANY>* in the list.

Don't forget to add a short description of your rule in the *Remark* field.

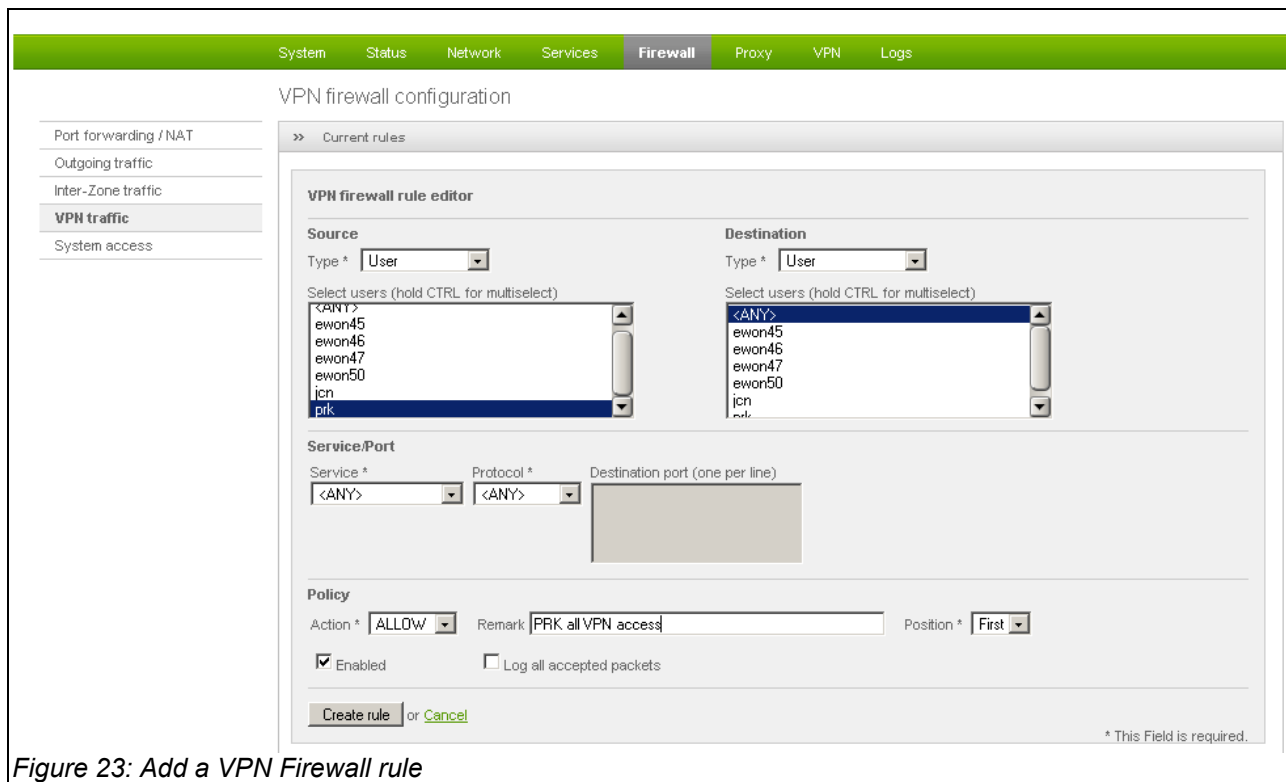


Figure 23: Add a VPN Firewall rule

And push the [Create rule](#) button.

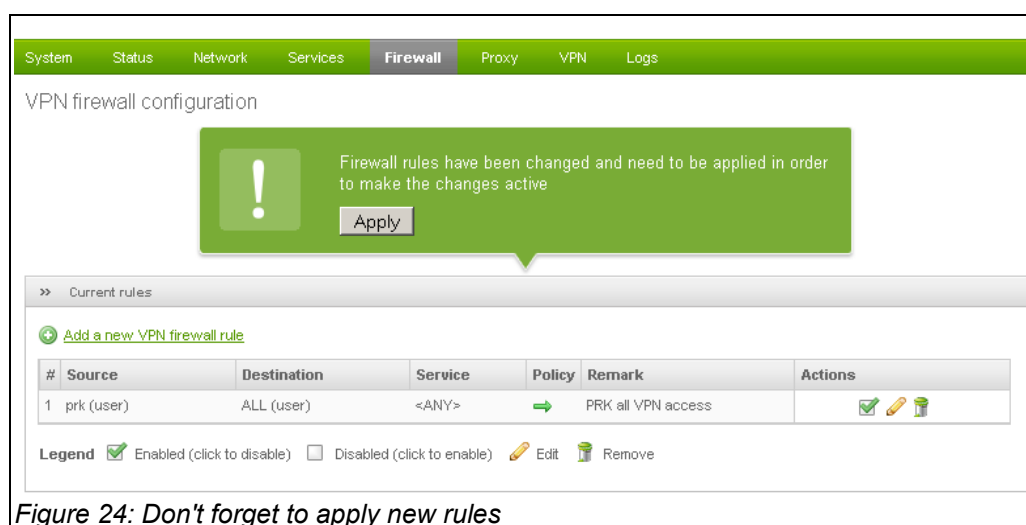


Figure 24: Don't forget to apply new rules

Use the Apply button to use immediately your new rule.

Create as many rules as required to build your *controlled* network.

Revisions

Revision Level	Date	Description
1.0	2009-01-22	First release.

- i Microsoft, Internet Explorer, Windows and Windows XP are either registered trademarks or trademarks of Microsoft Corporation
- ii Firefox is a trademark of the Mozilla Foundation

Document build number: 37

Note concerning the warranty and the rights of ownership:

The information contained in this document is subject to modification without notice. The vendor and the authors of this manual are not liable for the errors it may contain, nor for their eventual consequences.

No liability or warranty, explicit or implicit, is made concerning quality, the accuracy and the correctness of the information contained in this document. In no case the manufacturer's responsibility could be called for direct, indirect, accidental or other damage occurring from any defect of the product or errors coming from this document.

The product names are mentioned in this manual for information purposes only. The trade marks and the product names or marks contained in this document are the property of their respective owners.

This document contains materials protected by the International Copyright Laws. All reproduction rights are reserved. No part of this handbook can be reproduced, transmitted or copied in any way without written consent from the manufacturer and/or the authors of this handbook