

How to setup pfSense to act as OpenVPN server for Ewon devices

1 INTRODUCTION

The following document lists the different steps to configure pfSense to work as OpenVPN server in Bridged mode and how to connect Ewon devices to the pfSense.

The easiest way to connect an Ewon to pfSense is to configure the VPN server identical to an eFive VPN server. Like this, on the Ewon, to configure the VPN connection you can directly use the VPN wizard used also for eFive VPN connections.

Note: Using other settings for the OpenVPN server as those explained inside this document is also possible. This however will require to configure the Ewon by FTP and using additional VPN config files not covered inside this document.

Table of Contents

1	Introduction	1
2	Configuring pfSense to act as OpenVPN server in bridge mode.....	2
2.1	pfSense Interface configuration.....	2
2.2	OpenVPN server configuration	3
2.2.1	Create a CA (Certificate Authority)	3
2.2.2	Create a Server Certificate	3
2.2.3	Configure the VPN server.....	4
2.3	Check if the configuration is accepted and the server is running.....	6
2.4	Firewall Rules	6
2.5	Bridge the OpenVPN connection	7
2.5.1	Assign the Interface	7
2.5.2	Configure the assigned Interface	7
2.5.3	Declare the Bridge between VPN and LAN	7
2.6	Specify a VPN user for each Ewon	8
2.6.1	Create a VPN user for each Ewon	8
2.6.2	Specify fixed VPN-IP address for each Ewon	8
3	Configuring Ewon to connect to the OpenVPn server.....	9
4	Displaying connected devices on the OpenVPN server	10

2 CONFIGURING PFSense TO ACT AS OPENVPN SERVER IN BRIDGE MODE.

Following steps explain how to configure the pfSense to act identical as an Efive OpenVPN server.

We will use a typical Scada architecture as the one shown here under on an architecture used with an eFive.

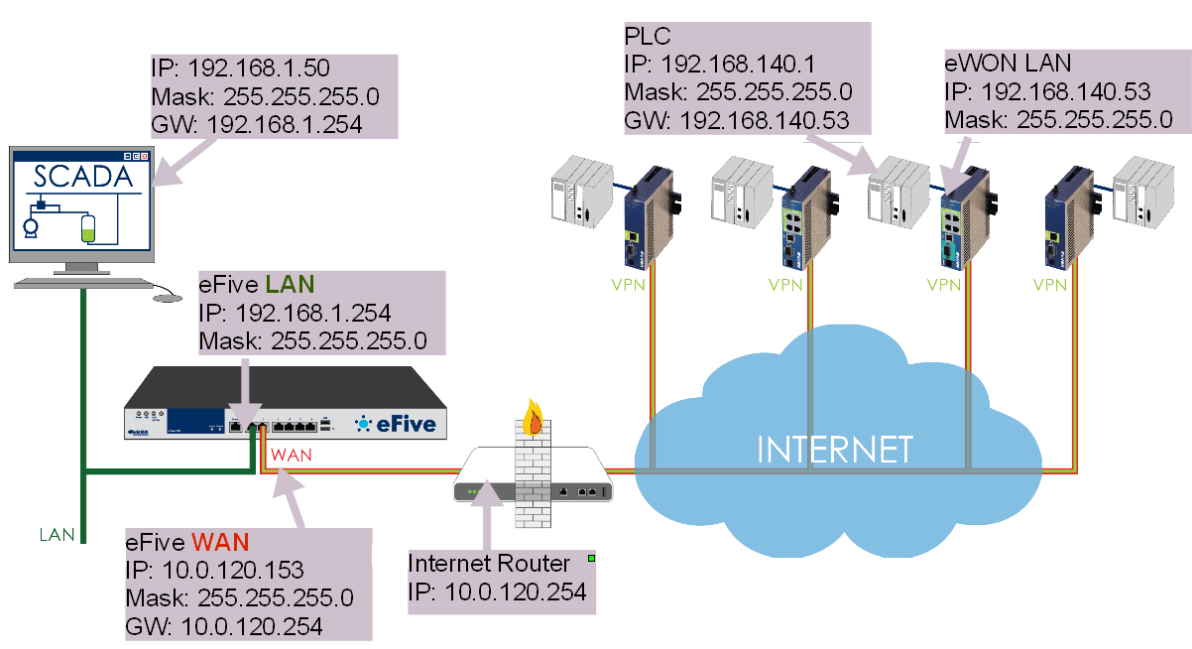


Figure 1

To perform this, we will need to configure the pfSense to act as VPN server in Bridge mode. OpenVPN offers the option of using tap interfaces and bridging clients directly onto the LAN or other internal network. This can make the remote clients appear to be on the local LAN.

2.1 PFSense INTERFACE CONFIGURATION

If not already done, configure the pfSense LAN and WAN interface. At first start of pfSense you'll be invited to run a wizard which will ask you those configurations.

If you want to change IP ranges afterwards, you can do it using the menu:

Interfaces / LAN

IPv4 Configuration Type: Static IPv4

IPv4 Address: 192.168.1.254 / 24

Interfaces / WAN

IPv4 Configuration Type: Static IPv4

Switch port: Port 1

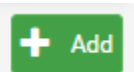
IPv4 Address: 10.0.120.153 / 24

IPv4 Upstream gateway: 10.0.120.254

2.2 OPENVPN SERVER CONFIGURATION

2.2.1 Create a CA (Certificate Authority)

System / Certificate Manager / CAs



Create / Edit CA

Descriptive name: VPNServer-CA (give a name to the CA)

Method: select "Create an internal Certificate Authority"

Internal Certificate Authority

Key length (bits): 2048

Digest Algorithm: sha1

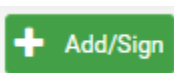
Lifetime (days): 3650

Common Name: VPNServer-CA (copy the CA name here)

Country Code, City, Organization: Optional info, but useful to identify the certificate

2.2.2 Create a Server Certificate

System / Certificate Manager / Certificates



Add/Sign a New Certificate

Method: select "Create an internal Certificate"

Descriptive name: VPNServer-Cert (give a name to the Cert)

Internal Certificate

Certificate authority: VPNServer-CA (select here the CA you just created before)

Key length (bits): 2048

Digest Algorithm: sha1

Lifetime (days): 3650

Common Name: VPNServer-Cert (or if you have a domain name for the public IP address used by your VPN server, enter it here)

Country Code, City, Organization: Optional info, but useful to identify the certificate

Certificate Attributes

Certificate Type: select "Server Certificate"

2.2.3 Configure the VPN server

VPN / OpenVPN / Servers



General Information

Server mode: select "Remote Access (User auth)"

Protocol: select "UDP on IPV4 only"

Device mode: select "tap – Layer 2 Tap Mode"

Interface: select "Wan"

Local port: 1194

Description: MyVPNServer (give a name to identify this instance of OpenVPN)

Cryptographic Settings

TLS Configuration: Uncheck the "use a TLS Key" option

Peer Certificate Authority: VPNServer-CA (the CA created in section 2.2.1)

Server certificate: VPNServer-Cert (the Cert created in section 2.2.2)

Encryption Algorithm: select "BF-CBC (128 bit key by default, 64 bit block)"

Enable NCP: Uncheck the "Enable Negotiable Cryptographic Parameters"

Auth digest algorithm: SHA1 (160-bit)

Tunnel Settings

IPv4 Tunnel Network: leave empty

Bridge DHCP: enable "Allow clients on the bridge to obtain DHCP."

Bridge Interface: select "LAN"

Concurrent connections: 200

Compression: select "LZO Compression"

Inter-client communication: [Optional]

If you want that VPN clients (Ewons and users) can communicate with each other, check the "Allow communication between clients connected to this server"

Server Bridge DHCP Start - Server Bridge DHCP End: [Optional]

If you want also to connect PCs to the OpenVPN server (so not an Ewon), you can use for those VPN client connections dynamically attributed VPN IP addresses. In this case you can define the range of IP-addresses used for those VPN users here

Client Settings

Dynamic IP: enable "Allow connected clients to retain their connections if their IP address changes."

Advanced Configuration

Custom options:

```
route-gateway "192.168.1.254";  
username-as-common-name;  
route 192.168.140.0 255.255.255.0 192.168.1.11;
```

Explication:

route-gateway "192.168.1.254" => to force client-generated traffic to be routed through the VPN tunnel (where 192.168.1.254 = LAN IP of pfSense)

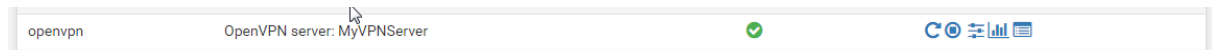
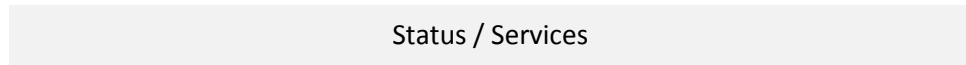
username-as-common-name => to allow specifying a fixed VPN address for each Ewon

route 192.168.140.0 255.255.255.0 192.168.1.12; => to allow reaching the network behind each Ewon (where 192.168.140/24 is the network behind the Ewon and 192.168.1.12 the VPN IP address of the eWON, see Figure 1)

add identical route for all Ewons if you want that the Scada can reach the devices connected to the Ewon LAN

Gateway creation: IPV4 only

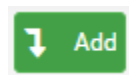
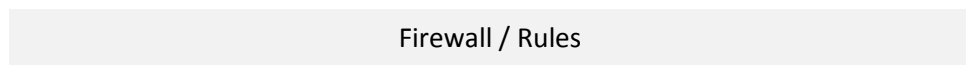
2.3 CHECK IF THE CONFIGURATION IS ACCEPTED AND THE SERVER IS RUNNING



Verify here if the VPN server you just created is up and running. A green check indicates that all is ok. If not you can open the related log entries link.

2.4 FIREWALL RULES

Now we need to open the firewall to allow incoming VPN connections on the WAN side of the pfSense.



[Edit Firewall rule](#)

Action: Pass

Interface: WAN

Address Family: IPv4

Protocol: UDP

Source

Source: any

Destination

Destination: WAN Address

Destination Port Range: OpenVPN (1194) (same port as configured inside VPN server)

Description: AllowOpenVPNOnWAN (specify a name to identify the Rule)



Save and:

2.5 BRIDGE THE OPENVPN CONNECTION

To finish the OpenVPN configuration in bridge mode, we need to link the VPN and LAN interface. For this we first need to assign an Interface to the VPN Network we just created.

2.5.1 Assign the Interface

Interface / Assignments / Interface Assignments

Select the VPN server you just created inside the available network ports and click on +Add



2.5.2 Configure the assigned Interface

Once the Interface created click on the Interface ('Opt3' for example) to open the configuration window:

Enable: check "Enable interface"

Description: MyOpenVPN (to easily identify the interface)

Click on "Save" and 

2.5.3 Declare the Bridge between VPN and LAN

Interface / Assignments / Bridges



Member Interfaces: select here the LAN and the MyOpenVpn interface just assigned before.

To select both interfaces, keep the control button pressed when selecting the interface with a mouse click.

Description: Vpn_LAN_bridge (to easily identify the bridge)

2.6 SPECIFY A VPN USER FOR EACH EWON

To allow the Scada system to reach the right Ewon or the network behind the Ewon, we need to use a fixed VPN-IP address for each Ewon.

2.6.1 Create a VPN user for each Ewon

System / User Manager / Users



Username: ewon001 (to identify the Ewon on the VPN network)

Password: Enter the password and confirm the password

Important: As for this VPN server configuration we use User Authentication, it is very important for security reasons to use here very strong passwords.

Perform identically for all other Ewons. For example ewon002, ewon003, etc.

2.6.2 Specify fixed VPN-IP address for each Ewon

VPN / OpenVPN/ Client Specific Overrides



General Information

Common Name: ewon001 (identical to the username created for the Ewon in section 2.6.1)

Client Settings

Advanced:

```
ifconfig-push 192.168.1.11 255.255.255.0;
```

Explication: define here the IP address that Ewon will receive for the VPN connection. Make sure the VPN address makes part of the LAN network of your pfSense, and that the IP address is not yet used on the network (by another LAN device or by another VPN client)

Perform identically for all other Ewons. For example, ewon002, ewon003, etc.

For ewon002 for example specify IP address 192.168.1.12, etc.

3 CONFIGURING EWON TO CONNECT TO THE OPENVPN SERVER

To configure each Ewon you'll need first to retrieve from the pfSense following info:

- the CA certificate (created in section 2.2.1, use the "Export CA" action to retrieve the CA)
- the username and password for the Ewon (created inside section 2.6.1)

To configure the Ewon flexy to connect to the pfSense Server, perform following steps:

Step1: Define the Lan IP address of the Ewon.

You can use the eBuddy software for easy LAN address configuration

Step2: Launch the system wizard

Allows to change the username and password and to specify the date and time settings of the Ewon.
Important: for security reason change the Ewon default password and use a strong password

Step3: Launch the Internet connection wizard

Select the interface you want to use for the Internet connection.

If you use the cabled Internet Wan connection, make sure to connect the WAN cable before launching the wizard.

Note: Your Flexy may dispose of an additional communication card (Wifi, 4G, etc.) .

Step4: Launch the VPN wizard

Select the "Configure eFive connectivity" option.

Server Address: the URL (or public IP address) on which the pfSense server can be reached

VPN Username & Password: the credentials for the Ewon created on the pfSense

CA Certificate: the CA certificate of the pfSense

Protocol: UDP

Port: 1194

The Ewon should now be connected to the VPN server.

The VPN cloud icon on the right bottom of the window should be displayed in green color.

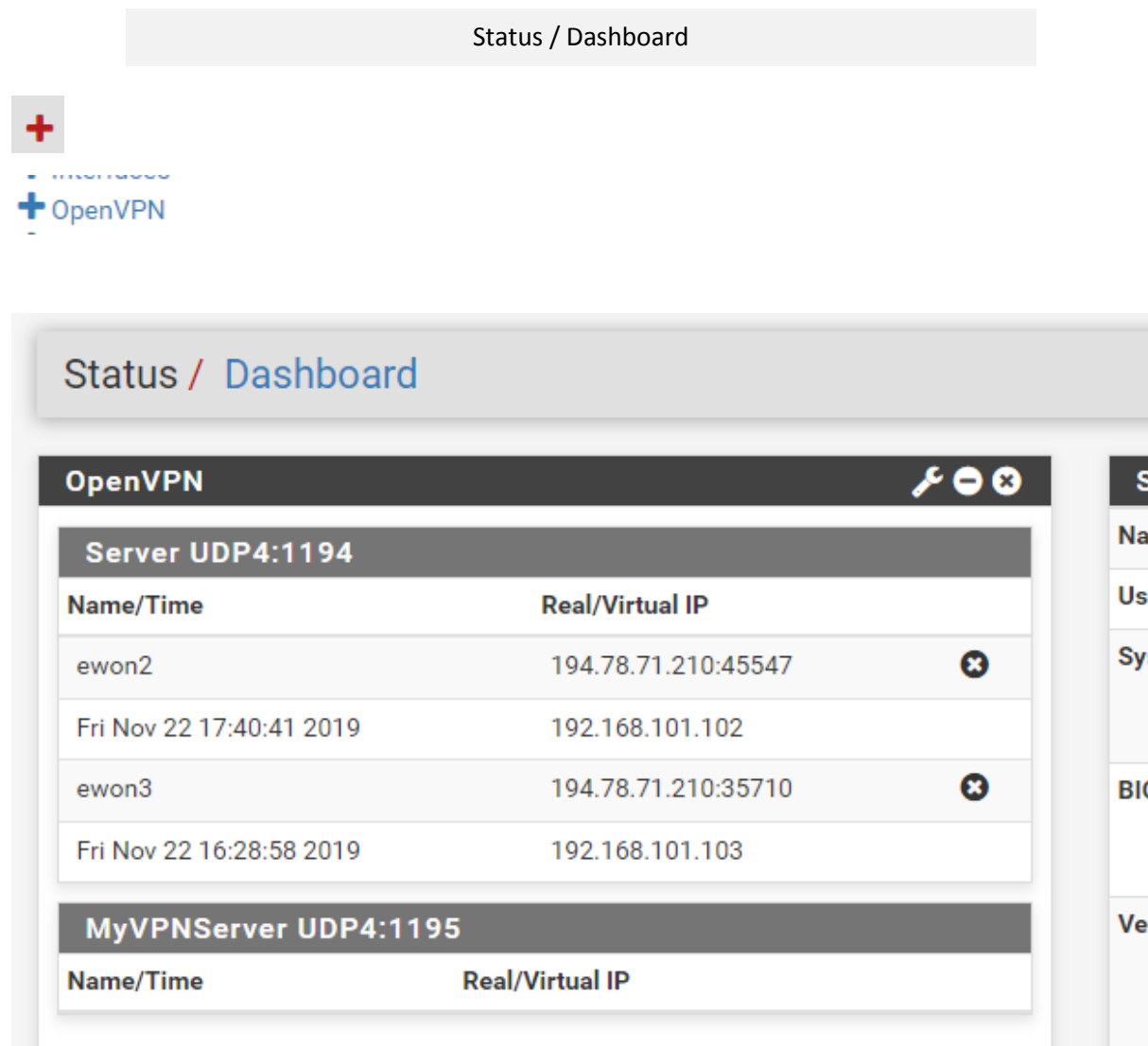
If not, best check inside the event log and realtime log of the Ewon, why the VPN connection failed.

Diagnostics / Logs / Event Logs

Diagnostics / Logs / Realtime Logs (to display the VPN connection logs)

4 DISPLAYING CONNECTED DEVICES ON THE OPENVPN SERVER

You can customize the pfSense dashboard (default page) to display the connected VPN users.



The screenshot shows the pfSense dashboard with the 'Status / Dashboard' header. A sidebar on the left contains a red plus icon and a blue plus icon next to the text 'OpenVPN'. The main content area displays a window titled 'OpenVPN' with a toolbar containing a key icon, a minus sign, and a close button. The window is divided into two sections: 'Server UDP4:1194' and 'MyVPNServer UDP4:1195'. The 'Server UDP4:1194' section contains a table with two columns: 'Name/Time' and 'Real/Virtual IP'. The table lists two active users: 'ewon2' with IP '194.78.71.210:45547' and 'Fri Nov 22 17:40:41 2019' with IP '192.168.101.102', and 'ewon3' with IP '194.78.71.210:35710' and 'Fri Nov 22 16:28:58 2019' with IP '192.168.101.103'. Each row has a small 'x' icon in the right margin. The 'MyVPNServer UDP4:1195' section is currently empty, showing only the column headers 'Name/Time' and 'Real/Virtual IP'.

Name/Time	Real/Virtual IP
ewon2	194.78.71.210:45547
Fri Nov 22 17:40:41 2019	192.168.101.102
ewon3	194.78.71.210:35710
Fri Nov 22 16:28:58 2019	192.168.101.103

Some other useful links to check the status of the OpenVPN server:

- OpenVPN status: [Status / OpenVPN](#)

Status / OpenVPN 🔍 📊 📄 ?

Server UDP4:1194 Client Connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent/Received	
ewon2 ewon2	194.78.71.210:45547	192.168.101.102	Fri Nov 22 17:40:41 2019	15.93 MiB / 13.36 MiB	✕
ewon3 ewon3	194.78.71.210:35710	192.168.101.103	Fri Nov 22 16:28:58 2019	12.65 MiB / 13.56 MiB	✕

Status: ✔ Actions: 🔄 🔍

+ Show Routing Table - Display OpenVPN's internal routing table for this server.

MyVPNServer UDP4:1195 Client Connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent/Received
-------------	--------------	-----------------	-----------------	---------------------

Status: ✔ Actions: 🔄 🔍

- Routes added on pfSense to reach Ewon LAN networks: [Diagnostic / routes](#)