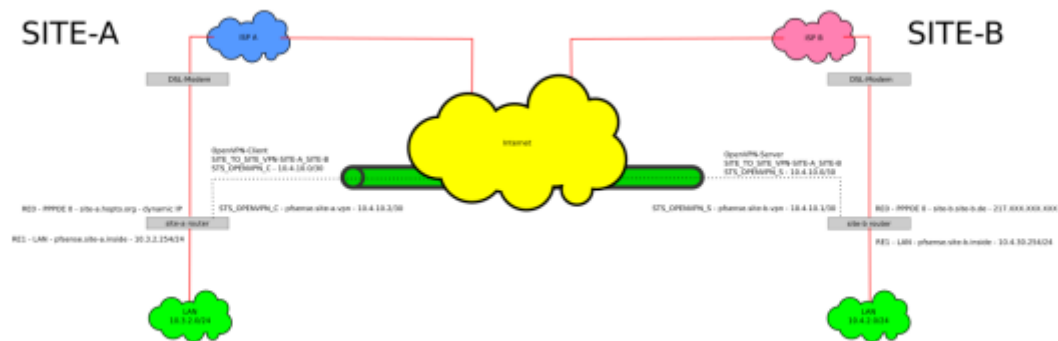


[openvpn](#), [pfsense](#), [sitetosite](#), [vpn](#), [apu1c4](#), [pcengines](#)

## simple site to site VPN with pfSense and OpenVPN

I just had to set up a simple site to site VPN between a site with a fixed IP (SITE-B) and a site with a dynamic IP (SITE-A). Both routers are running the 'Community Edition' of [pfSense](#) and are installed on [PC Engines APU.1C4](#). I have followed the documentation at [pfSense.org](#) about how to [configure a Site To Site VPN with OpenVPN](#) to get the VPN up and running. Because some things aren't documented there I will put up my own HowTo here. Please do yourself a favour and read the [documentation at pfsense.org](#) first because it explains things in more detail than I will do here.



This HowTo will guide you through the setup of:

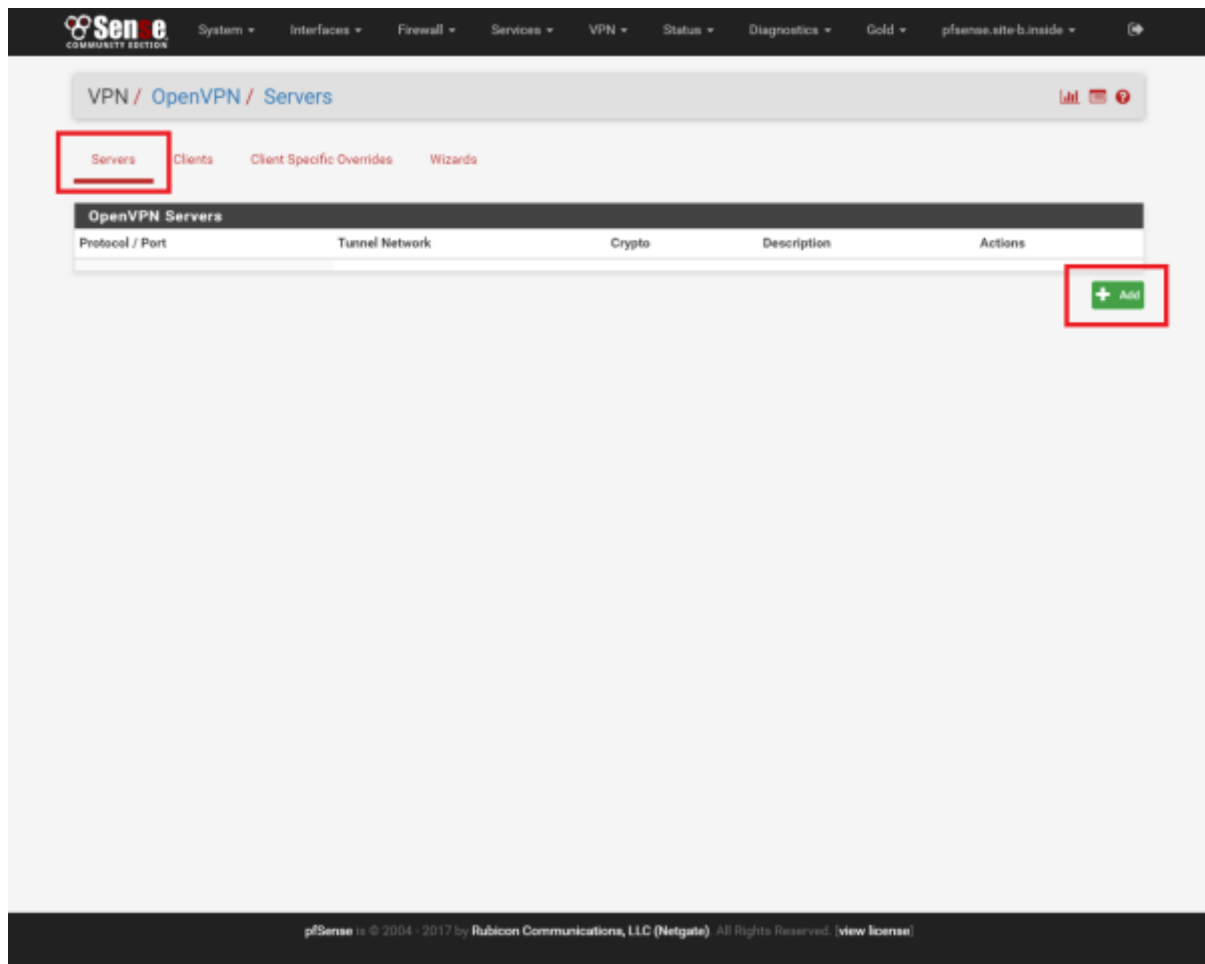
- An IPv4 'Site To Site VPN' with [OpenVPN](#) on the pfSense platform (2.3.4 at time of writing) as seen in the schema above with the specific settings for the PC Engines APU hardware platform.
- The client will autoconnect to the server and (in the event of disconnection) reconnect automatically.
- The authentication between the client and the server will happen automatically via pre-shared key.

## Sources


- [pfsense.org - OpenVPN Site To Site](#)
- [The pfSense Book](#)

## Configure the OpenVPN server on SITE-B router

- Navigate to 'VPN - OpenVPN'



- On the '**Servers**'-Tab click on the '**+ Add**'-button to add a new server


System ▾
Intraces ▾
Firewall ▾
Services ▾
VPN ▾
Status ▾
Diagnostics ▾
Gold ▾
pfSense site-b inside ▾

VPN / OpenVPN / Servers / Edit

Servers
Clients
Client Specific Overrides
Wizards

General Information

**Disabled**
☐ Disable this server  
Set this option to disable this server without removing it from the list.

**Server mode**
Peer to Peer ( Shared Key )

**Protocol**
UDP

**Device mode**
tun

**Interface**
WAN

**Local port**
1194

**Description**
Site\_To\_Site-SITE-A\_SITE\_B  
A description may be entered here for administrative reference (not parsed).

Cryptographic Settings

**Shared key**
☒ Automatically generate a shared key

**Encryption Algorithm**
AES-256-CBC (256 bit key, 128 bit block)

**Auth digest algorithm**
RSA-SHA512 (512-bit)  
Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.

**Hardware Crypto**
No Hardware Crypto Acceleration

Tunnel Settings

**IPv4 Tunnel Network**
10.4.10.0/30  
This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).

**IPv6 Tunnel Network**  
This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. fe80::/64). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).

**IPv4 Remote network(s)**
10.3.2.0/24  
IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

**IPv6 Remote network(s)**  
These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

**Concurrent connections**
1  
Specify the maximum number of clients allowed to concurrently connect to this server.

**Compression**
Enabled with Adaptive Compression  
Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.

**Type-of-Service**
☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

**Duplicate Connection**
☐ Allow multiple concurrent connections from clients using the same Common Name.  
(This is not generally recommended, but may be needed for some scenarios.)

**Disable IPv6**
☒ Don't forward IPv6 traffic.

Advanced Configuration

**Custom options**  
  
Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.  
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

**Verbosity level**
default  
Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.  
None: Only fatal errors  
Default through 4: Normal usage range  
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.  
6-11: Debug info range

Save

pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license](#)

- In the '**General Information**'-section:
  - **Disable this server:** ☐
  - **Server mode:** Peer to Peer (Shared Key)
  - **Protocol:** UDP
  - **Device Mode:** tun
  - **Interface:** set it to whatever external interface you want to have your OpenVPN server listening on. In my case this is 'WAN'.
  - **Local port:** set it to the port you want the local OpenVPN server to listen on. Default is '1194'.
  - **Description:** Set an appropriate description e.g. 'Site\_To\_Site-SITE-A\_SITE\_B'
- In the '**Cryptographic Settings**'-section:
  - **Automatically generate a shared key:** ☒
  - **Encryption Algorithm:** AES-256-CBC (256 bit key, 128 bit block)
  - **Auth digest algorithm:** RSA-SHA512 (512-bit)
  - **Hardware Crypto:** No Hardware Crypto Acceleration (this is PC Engines APU specific, if your hardware has crypto support - enable it)
- In the '**Tunnel Settings**'-Section:
  - **IPv4 Tunnel Network:** 10.4.10.0/30 (this a very small subnet with 2 useable IP addresses since there is only one server and one client)
  - **IPv6 Tunnel Network:** leave empty
  - **IPv4 Remote network(s):** 10.3.2.0/24 (this is a comma separated list for all the networks you want to connect to on the client side (SITE A))
  - **IPv6 Remote network(s):** leave empty
  - **Concurrent connections:** 1
  - **Compression:** Enabled with Adaptive Compression
  - **Type-of-Service:** ☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value
  - **Duplicate Connection:** ☐ Allow multiple concurrent connections from clients using the same Common Name
  - **Disable IPv6:** ☒ Don't forward IPv6 traffic
- In the '**Advanced Configuration**'-section:
  - Custom options: leave empty
  - Verbosity Level: default
- Click on 'Save'-button

You should now be forwarded to the list with your configured OpenVPN servers under '**VPN - OpenVPN**' on the '**Servers**'-tab

From:  
<https://wiki.nanoscopic.de/> - nanoscopic wiki

Permanent link:  
<https://wiki.nanoscopic.de/doku.php/pages/howtos/pfsense/simple-site-to-site-vpn-with-pfsense-and-openvpn?rev=1615746068>

Last update: 2021/03/14 18:21

