Автор:
14.01.13 17:39 - Последнее обновление 14.01.13 17:41

OpenVPN with Site to Site Routing

Connecting two sites using OpenVPN is very simple. One side is configured as a client, and the other as a server. Usually with site to site connections you want to use shared keys.

The instructions below are for basic site to site connectivity. For advanced options/configurations see the Advanced Options Section below and the pfSense book . For other modes such as SSL/TLS, or remote access, look in the Category:OpenVPN OpenVPN category of the doc wiki.

This document only covers pfSense 2.0. For 1.2.3, see OpenVPN Site To Site .

Info

You can have both IPSec and OpenVPN enabled/in use at the same time, however, not for the same subnets. Any IPSec tunnel that references the same pair of subnets you wish to use in OpenVPN must be disabled, but IPSec and OpenVPN do not conflict.

The way OpenVPN works is that one end of the tunnel needs to be the “server” and the other the “client”, it does not matter which, though if doing more than one site, you should have the main site as the “server”.

You must create a firewall rule on the Server's WAN interface to allow traffic through to the interface and port where the server is running, otherwise the traffic will be blocked and the VPN will fail to connect. To allow or filter incoming traffic inside the VPN tunnel, add rules to the OpenVPN tab under Firewall > Rules.

OpenVPN in shared key mode is the recommend method for site to site connections, unless you have a half dozen or more sites. For PKI and advanced options/configurations see OpenVPN Site-to-Site PKI (SSL) and the pfSense book

.

For more than 5 connections site to site or roadwarrior VPNs you probably want to use SSL/TLS (PKI) for ease of management.

Server Settings

Go to VPN > OpenVPN you will be on the server page by default, click the + symbol

Server Mode : Peer to Peer (Shared Key)

Protocol : UDP - TCP is undesirable because every packet is retransmitted that is lost, and if its using TCP, it will be retransmitted anyway. This would slow down the VPN if you have a lot of lost traffic on the WAN connection. TCP is really only useful if you need to bypass firewalls, in which case your port should be 443 as almost no one blocks this one. Must match on each side. If you choose port 443, ensure the WebGUI is not running on that port first.

Device Mode : tun

Interface : Whichever interface you want the server to use for incoming connections. Typically WAN, but may be an OPT WAN. You may also use "any" and then it will bind to all interfaces.

Local Port : The port this OpenVPN server will listen on. 1194 is the default OpenVPN port. Each server requires a unique port. Make sure not to use a port in use by another service otherwise problems can occur.

Description : A name for this VPN. Shows up in various places where you can select the VPN from a list, such as Status > Services, or Diagnostics > Packet Capture.

Shared key : On 2.0, the keys can be made in the GUI. You can check "Automatically generate a shared key.", and when the settings are saved, a key will be generated for you. You can then copy/paste the key into the client.

Encryption algorithm : This setting must match on both sides. Any of the crypto options are fine, it depends on the user preference. If you are on ALIX, you should use aes-128-cbc, see this wiki
For most others, aes-256-cbc is good, or whatever you like. CAST/DES/RC2 may be less secure, but are also faster.

Hardware Crypto : If your device has hardware crypto support, you can choose it from this list. For ALIX and many others, use "BSD cryptodev engine" to use supported onboard devices.

Tunnel Network : The suggested default in the GUI of 10.0.8.0/24 is sufficient, but really recommend using any random unused network inside of the RFC1918 space. For site-to-site shared key, you really only need a /30, not a /24.

Remote network : Enter the remote (Client Side) LAN here, to access more than one network, use the custom options field, for more info please see Advanced Options section below and the pfSense book .

Compression : Check this if you want to compress data on the tunnel. If you primarily transfer bulk data or encrypted protocols like https/ssh, this may only add unnecessary overhead.

Type-of-Service : Set the TOS IP header value of tunnel packets to match the encapsulated packet value. Useful if you want to do traffic shaping on the OpenVPN traffic itself, but it does expose some data about the contents of the packet, so it is a potential security risk.

Firewall Rules : Don't forget to add a firewall rule on the WAN tab under Firewall > Rules (or whichever interface the server is running on) to allow traffic to reach the OpenVPN server's IP:port where it's listening. Also don't forget rules on the OpenVPN tab to allow traffic inside the tunnel.

Client Settings

Go to VPN > OpenVPN You will be on the server page by default, click Clients tab, and then the + symbol.

Server Mode : Peer to Peer (Shared Key)

Protocol : Match the setting from the server side.

Device Mode : tun

Interface : Whichever interface you want the server to use for outbound traffic. Typically WAN, but may be an OPT WAN. You may also use "any" and then it will bind to all interfaces.

Local Port : Leave this blank for a random port. The port this OpenVPN client will use for its side (source port). 1194 is the default OpenVPN port. Each process requires a unique port. Make sure not to use a port in use by another service otherwise problems can occur.

Server host or address: FQDN (vpn.example.com) or IP (69.64.6.21)

Server Port: The port the OpenVPN client will connect to on the Server

Description : A name for this VPN. Shows up in various places where you can select the VPN from a list, such as Status > Services, or Diagnostics > Packet Capture.

Shared key : Copy/paste the key from the server.

Encryption algorithm : Match the setting from the server side.

Hardware Crypto : If your device has hardware crypto support, you can choose it from this list. For ALIX and many others, use "BSD cryptodev engine" to use supported onboard devices.

Tunnel Network : The suggested default in the GUI of 10.0.8.0/24 is sufficient, but really recommend using any random unused network inside of the RFC1918 space. For site-to-site shared key, you really only need a /30, not a /24.

Remote network : Enter the remote (Server Side) LAN here, to access more than one network, use the custom options field, for more info please see Advanced Options section below and the pfSense book .

Compression : Match the setting from the server side.

Type-of-Service : Set the TOS IP header value of tunnel packets to match the encapsulated packet value. Useful if you want to do traffic shaping on the OpenVPN traffic itself, but it does expose some data about the contents of the packet, so it is a potential security risk.

Firewall Rules : Don't forget to add rules to Firewall > Rules on the OpenVPN tab to allow traffic inside the tunnel.

Advanced Options

To access additional networks, you add a route to the side opposite where the network is located. For example, to access 172.18.4.0/24, which resides on the server side, add the following custom option:

```
route 172.18.4.0 255.255.255.0;
```

Автор:
14.01.13 17:39 - Последнее обновление 14.01.13 17:41

источник: http://doc.pfsense.org/index.php/OpenVPN_Site-to-Site_%28Shared_Key,_2.0%29
ссылка на материал: http://www.thin.kiev.ua/router-os/50-pfsense/745-openvpn-site-to-site-shared-key-20.html
{jcomments on}