Site-to-Site OpenVPN with routes

Install

https://github.com/angristan/openvpn-install

First, get the script and make it executable :

```
curl -O https://raw.githubusercontent.com/Angristan/openvpn-install/master/openvpn-install.sh
chmod +x openvpn-install.sh
```

Then run it :

```
./openvpn-install.sh
```

Make 2 clients, one called **client01** and the other called **client02**

Then edit server conf and add belllow:

/etc/openvpn/server.conf

```
client-config-dir /etc/openvpn/ccd
push "route 192.168.2.0 255.255.255.0"
route 192.168.2.0 255.255.255.0 10.8.0.2
client-to-client
```

/etc/openvpn/ccd/client01

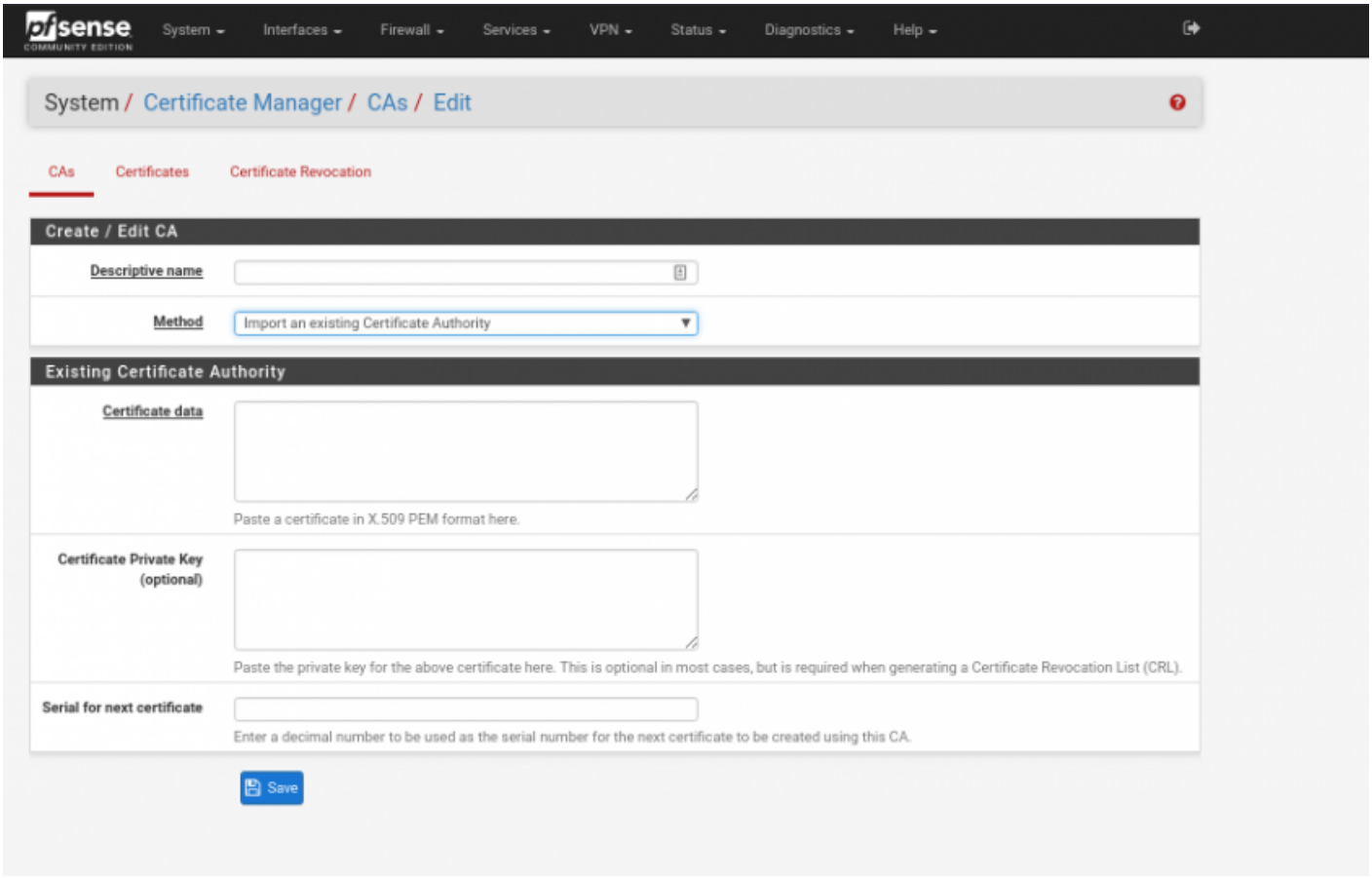
```
iroute 192.168.2.0 255.255.255.0
```

/etc/openvpn/ccd/client02

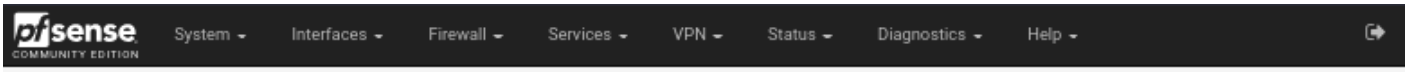
```
iroute 10.1.2.0 255.255.255.0
```

Pfsense Example

import cert



Add Client



VPN / OpenVPN / Clients / Edit

Servers | Clients | Client Specific Overrides | Wizards | Client Export | Shared Key Export

General Information

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

Server mode
Peer to Peer (SSL/TLS)

Protocol
UDP on IPv4 only

Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Interface
WAN
The interface used by the firewall to originate this OpenVPN client connection

Local port
1194
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.

Server host or address
The IP address or hostname of the OpenVPN server.

Server port
1194
The port used by the server to receive client connections.

Proxy host or address
The address for an HTTP Proxy this client can use to connect to a remote server.
TCP must be used for the client and server protocol.

Proxy port

Proxy Authentication
none
The type of authentication used by the proxy server.

Description
A description may be entered here for administrative reference (not parsed).

User Authentication Settings

Username
Leave empty when no user name is needed

Password
Password
Leave empty when no password is needed
Password
Confirm

Authentication Retry
☑ Do not retry connection when authentication fails
When enabled, the OpenVPN process will exit if it receives an authentication failure message. The default behavior is to retry.

Cryptographic Settings

TLS Configuration
☑ Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.

TLS Key
```
-----BEGIN OpenVPN Static key V1-----
f60b6b581f35ed939230e1875df97865
a4f39ca227aac59fcbb0e05b735469f6
1daa2a07f38c3903ec8193678b0fb854
0c6257c1dca0012d3e7fb5552c9bd6c9
```
Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode
TLS Encryption and Authentication
In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

Peer Certificate Authority
openvpn-do

Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation

Client Certificate

Revocation list

Client Certificate: openvpn-docrt (CA: openvpn-do, In Use)

Encryption Algorithm: AES-128-GCM (128 bit key, 128 bit block)

The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.

Enable NCP: Enable Negotiable Cryptographic Parameters

Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below.

NCP Algorithms

Available NCP Encryption Algorithms:
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)

Click to add or remove an algorithm from the list

Allowed NCP Encryption Algorithms:
AES-128-GCM

Click an algorithm name to remove it from the list

The order of the selected NCP Encryption Algorithms is respected by OpenVPN.

Auth digest algorithm: SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
Set this to the same value as the server. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto: No Hardware Crypto Acceleration

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24). The second usable address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

IPv6 Tunnel Network

This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

IPv4 Remote network(s)

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.

Limit outgoing bandwidth: Between 100 and 100,000,000 bytes/sec

Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second). Not compatible with UDP Fast I/O.

Compression: Omit Preference (Use OpenVPN Default)

Compress tunnel packets using the LZO algorithm.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

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.

Topology: Subnet -- One IP address per client in a common subnet

Specifies the method used to configure a virtual adapter IP address.

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

Don't pull routes: Bars the server from adding routes to the client's routing table

This option still allows the server to set the TCP/IP properties of the client's TUN/TAP interface.

Don't add/remove routes: Don't add or remove routes automatically

Do not execute operating system commands to install routes. Instead, pass routes to --route-up script using environmental variables.

Advanced Configuration

Custom options

```
persist-key;
persist-tun;
verify-x509-name server_F5vhaIOmfpNlch5d name;
remote-cert-tls server;
```

Set this to the same value as the server. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto: No Hardware Crypto Acceleration

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24). The second usable address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

IPv6 Tunnel Network

This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

IPv4 Remote network(s)

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.

Limit outgoing bandwidth: Between 100 and 100,000,000 bytes/sec

Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second). Not compatible with UDP Fast I/O.

Compression: Omit Preference (Use OpenVPN Default)

Compress tunnel packets using the LZO algorithm.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

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.

Topology: Subnet -- One IP address per client in a common subnet

Specifies the method used to configure a virtual adapter IP address.

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

Don't pull routes: ☐ Bars the server from adding routes to the client's routing table

This option still allows the server to set the TCP/IP properties of the client's TUN/TAP interface.

Don't add/remove routes: ☐ Don't add or remove routes automatically

Do not execute operating system commands to install routes. Instead, pass routes to --route-up script using environmental variables.

Advanced Configuration

Custom options

```
persist-key;
persist-tun;
verify-x509-name server_F5vhaIOmfpNlch5d name;
remote-cert-tls server;
tls-client;
tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256;
tls-version-min 1.2;
auth-nocache;
verb 3;
```

Enter any additional options to add to the OpenVPN client configuration here, separated by semicolon.

UDP Fast I/O: ☑ Use fast I/O operations with UDP writes to tun/tap. Experimental.

Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

Send/Receive Buffer: Default

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

Gateway creation: ◉ Both ○ IPv4 only ○ IPv6 only

If you assign a virtual interface to this OpenVPN client, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level: 3 (recommended)

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

Revision #5
Created 2018-05-06 19:44:08 UTC by Dave
Updated 2019-09-17 04:04:32 UTC by Dave