Edit

Servers | Clients | Client Specific Overrides | Wizards

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

TCP 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

0

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

Server host or address

146.70.61.130

The IP address or hostname of the OpenVPN server.

Server port

443

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

AirVPN_GB-London_Carinae_TCP-443

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

User Authentication Settings

Username

Leave empty when no user name is needed

Password

Leave empty when no password is needed

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-----
:]
-----END OpenVPN Static key V1-----
```

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.

TLS keydir direction

Direction 1

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority

AirVPN_CA

Peer Certificate Revocation list

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

Client Certificate

AirVPN_GB-London_Carinae_TCP-443 (CA: AirVPN_CA, In Use)

Data Encryption Negotiation

☑ Enable Data Encryption Negotiation

This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

Data 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)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

AES-256-GCM

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

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

Fallback Data Encryption Algorithm

AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation. This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm

SHA512 (512-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

Intel RDRAND engine - RAND

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.

Allow Compression

Refuse any non-stub compression (Most secure)

Allow compression to be used with this VPN instance.
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.

Asymmetric compression allows an easier transition when connecting with older peers.

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.

Pull DNS

□ Add server provided DNS

If this option is set, pfSense will use DNS servers assigned by remote OpenVPN server for its own purposes (including the DNS Forwarder/DNS Resolver).

Ping settings

Inactive

0

Causes OpenVPN to exit after n seconds of inactivity on the TUN/TAP device.
The time length of inactivity is measured since the last incoming or outgoing tunnel packet.
0 disables this feature.

Ping method

keepalive -- Use keepalive helper to define ping configuration

keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
ping = interval
ping-restart = timeout

Interval

5

Timeout

30

Advanced Configuration

Custom options

```
client;persist-key;persist-tun;remote-cert-tls server;prng sha256
64;mlock;auth-nocache;
```

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

Send/Receive Buffer

512 KiB

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

4

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