Edit

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

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 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 or Virtual IP address where OpenVPN will receive client connections.

Local port

1194

The port used by OpenVPN to receive client connections.

Description

S2S to OpenWRT example VPN

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

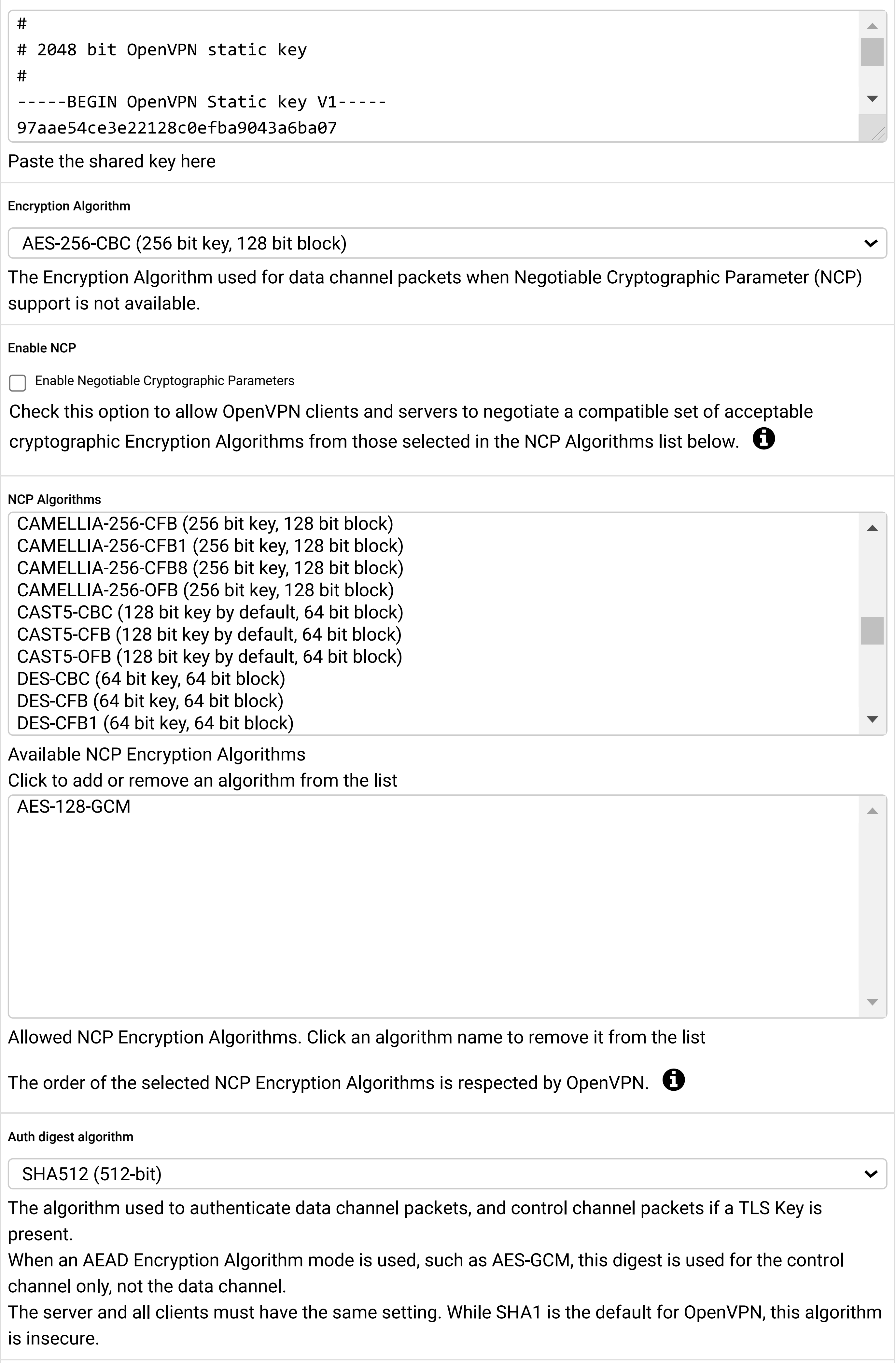
Cryptographic Settings

TLS keydir direction

Use default direction

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.

Shared Key



```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
97aae54ce3e22128c0efba9043a6ba07
```

Paste the shared key here

Encryption Algorithm

AES-256-CBC (256 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

CAMELLIA-256-CFB (256 bit key, 128 bit block)
CAMELLIA-256-CFB1 (256 bit key, 128 bit block)
CAMELLIA-256-CFB8 (256 bit key, 128 bit block)
CAMELLIA-256-OFB (256 bit key, 128 bit block)
CAST5-CBC (128 bit key by default, 64 bit block)
CAST5-CFB (128 bit key by default, 64 bit block)
CAST5-OFB (128 bit key by default, 64 bit block)
DES-CBC (64 bit key, 64 bit block)
DES-CFB (64 bit key, 64 bit block)
DES-CFB1 (64 bit key, 64 bit block)

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

AES-128-GCM

Allowed NCP Encryption Algorithms. 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

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.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto

No Hardware Crypto Acceleration

Tunnel Settings

IPv4 Tunnel Network

10.63.51.0/24

This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network

This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

IPv4 Remote network(s)

192.168.239.0/24

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

Specify the maximum number of clients allowed to concurrently connect to this server.

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.

Type-of-Service

☑ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

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*2
push ping = interval
push ping-restart = timeout

Interval

10

Timeout

60

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"

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.

Exit Notify

Disabled

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. In Peer-to-Peer Shared Key or with a /30 Tunnel Network, this value controls how many times this instance will attempt to send the exit notification.

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 server, this setting controls which gateway types will be created. The default setting is 'both'.

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