VPN / OpenVPN / Servers / 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
Remote Access (SSL/TLS + User Auth)

Backend for authentication
Local Database

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

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

pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
c32239958bf2d76762ecf07dca578ad3
```

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 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	COL
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
Server certificate	COLVPN (Server: Yes, CA: COL, In Use)
DH Parameter Length	2048 bit Diffie-Hellman (DH) parameter set used for key exchange. ℹ
ECDH Curve	Use Default The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Encryption Algorithm	AES-128-CBC (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. ℹ
NCP 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)	AES-128-GCM
Available NCP Encryption Algorithms Click to add or remove an algorithm from the list	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. ℹ

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.
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

Certificate Depth

Two (Client+Intermediate+Server)

When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Strict User-CN Matching

☐ Enforce match

When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

Tunnel Settings

IPv4 Tunnel Network

10.0.8.0/24

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.

Redirect IPv4 Gateway	☑ Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	☐ Force all client-generated IPv6 traffic through the tunnel.
IPv6 Local network(s)	IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent connections	4 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.
Push Compression	☐ Push the selected Compression setting to connecting clients.
Type-of-Service	☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	☑ Allow communication between clients connected to this server
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.)

Client Settings

Dynamic IP	☑ Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet – One IP address per client in a common subnet Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Advanced Client Settings

DNS Default Domain	☐ Provide a default domain name to clients
DNS Server enable	☑ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	192.168.1.100
DNS Server 2	8.8.8.8
DNS Server 3	
DNS Server 4	
Block Outside DNS	☑ Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Force DNS cache update	☐ Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable	☐ Provide an NTP server list to clients
NetBIOS enable	☑ Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
Node Type	none Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast)
Scope ID	 A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID
WINS server enable	☐ Provide a WINS server list to clients

Advanced Configuration

Custom	

options	`push "route 192.168.1.0 255.255.255.0"` 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.
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	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 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