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
1195
The port used by OpenVPN to receive client connections.

Description
OPENVPN-[redacted]
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
```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
11ebb5c3ede6954dff843bfea8c9ce18
```
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.

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.

Peer Certificate Authority
[redacted]

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

OCSP Check
☐ Check client certificates with OCSP

Server certificate
[redacted]

DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.

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.

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
0 Objekte | 0 Objekte
Available Data Encryption Algorithms
Click to add or remove an algorithm from the list
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
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
One (Client+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
192.168.81.0/24
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.

IPv4 Local network(s)
192.168.101.0/24
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. 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.

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
20
Specify the maximum number of clients allowed to concurrently connect to this server.

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.

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 the same user
When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

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".

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 Client Settings

DNS Default Domain
☑ Provide a default domain name to clients

DNS Default Domain
[redacted]

DNS Server enable
☑ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1
192.168.101.101

DNS Server 2

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.

Advanced Configuration

Custom options
```
push "dhcp-option DNS 192.168.101.101";
push "route 192.168.4.1 255.255.255.0";
push "route 192.168.81.1 255.255.255.0";
push "route 192.168.101.101 255.255.255.0";
push "route 192.168.101.101 255.255.255.0";
```
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"

Username as Common Name
☑ Use the authenticated client username instead of the certificate common name (CN).
When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.

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