Specification

Basic Capabilities of SoftEther VPN Server

Maximum Concurrent VPN Sessions

- 4,096 Sessions

Maximum Virtual Hubs

- 4,096 Virtual Hubs

Remote Access VPN

- Layer-2 (Ethernet Bridging)
- Layer-3 (IP Routing)

Site-to-Site VPN

- Layer-2 (Ethernet Bridging)
- Layer-3 (IP Routing)

Traffic Control

- VoIP / QoS Priority Control
- Traffic Shaping for Per Users or Groups

Maximum Objects in a Virtual Hub

- Users: 10,000
- Groups: 10,000
- Access List Entries: 32,768
- MAC Address Table Entries: 65,536
- IP Address Table Entries: 65,536
- Cascade Connections: 128

SecureNAT Function

- Virtual NAT Function: Maximum 4,096 Dynamic Mapping
- User-mode NAT
- Kernel-mode NAT
- Virtual DHCP Function

High Availability and Clustering

- Maximum Cluster Members: 64
- Load Balancing
- Load Balancing Weight Control
- Dynamic Mode Virtual Hub Mapping over Cluster Members
- Static Mode Virtual Hub Mapping over Cluster Members
- Fault Tolerance

Security Features

- External User-authentication Methods: RADIUS / NT Domain / Active Directory
- Security Policy Settings for Per User / Per Group
- Security Logs Isolation for Each Virtual Hubs
- Works as System-mode Background Service
- Works as User-mode Program
- DoS Attacks Detection and Protection (SYN Flood)

Management Functions

- VPN Server Manager GUI for Windows
- Command-line Management Utility (vpncmd)
- Listener Ports Dynamic Add / Delete

VPN Protocols Supported by SoftEther VPN Server

- SoftEther VPN Protocol (Ethernet over HTTPS)
- OpenVPN (L3-mode and L2-mode)
- L2TP/IPsec
- MS-SSTP (Microsoft Secure Socket Tunneling Protocol)
- L2TPv3/IPsec
- EtherIP/IPsec

SoftEther VPN Protocol Specification

- Supported Payload Protocols: Any Protocols in Ethernet
- Upper Underlying Protocol: SSL (Secure Socket Layer) 3.0 / TLS (Transport Layer Security) 1.0
- Lower Underlying Protocol: TCP/IP and UDP/IP Hybrid (on IPv4 and IPv6)
- Ciphers:
  RC4-MD5, RC4-SHA, AES128-SHA, AES256-SHA, DES-CBC-SHA and DES-CBC3-SHA
- Data Compression: zlib
- Session-key: 128bit

- Based Standards: Extended HTTPS over SSL Protocol (RFC2818, RFC 5246)
- WAN Optimization: 1-32 Parallel TCP Connection to Construct a Logical VPN Session
- Persistent Link: Infinite Auto-reconnect Function
- Proxy Support: HTTP Proxy Server and SOCKS Proxy Server
- TCP Ports: 443, 992 and 5555 is Listening by Default.
  You can add/delete listening TCP ports.
- Behind NAT Solution:
  NAT-Traversal Function is enabled by default. No need to open any TCP/UDP ports on the NAT for accepting VPN connections which are initiated from Internet-side.
- Anti-restricted Firewall Solution:
  VPN over ICMP (Encapsulate all Ethernet packets over ICMP packets)
  VPN over DNS (Encapsulate all Ethernet packets over DNS packets)
- User-authentication:
  - Anonymous
  - Standard Password Authentication
  - Password Authentication for RADIUS
  - Password Authentication for NT Domain and Active Directory
  - X.509 RSA PKI Certification Authentication (Key file on Disk)
  - X.509 RSA PKI Certification Authentication (PKCS#11 Smart-cards or USB Tokens)
- VPN Encapsulation Payload:
  Ethernet (IEEE802.3) Frames (Up to 1,514bytes or 1,518bytes for IEEE802.1Q VLAN Tags)
- Supported VPN Clients: SoftEther VPN Client
- Supported Client OS: Windows and Linux
- Supported VPN Topologies: Remote-access VPN, Site-to-Site VPN (L2-Bridging) and Site-to-Site VPN (L3-Routing)

L2TP/IPsec Sever Function Specifications on SoftEther VPN Server

- User-authentication Methods: PAP and MS-CHAPv2
- NAT-Traversal: RFC3947 IPsec over UDP Encapsulation
- Transport UDP Ports:
  UDP 500 and 4500
  (Allow both ports on the firewall. Add UDP port forwarding for both 500 & 4500 on the NAT.)
- Supported Ciphers:
  DES-CBC, 3DES-CBC, AES-CBC, Blowfish-CBC and CAST-128-CBC
- Supported Hashes:
  MD5 and SHA-1
- Supported Diffie-Hellman Groups:
  MODP 768 (Group 1), MODP 1024 (Group 2) and MODP 1536 (Group 5)

- Compatible VPN Clients: Built-in VPN Clients on Windows, Mac, iOS and Android
- Compatible Client OS: Windows, Mac, iOS, Android and other L2TP-supported VPN Client OS
- Supported VPN Topologies: Remote-access VPN

OpenVPN Server Function Specifications on SoftEther VPN Server

- OpenVPN Clone Function for Compatibility with OpenVPN Technologies, Inc.'s implementation.
- Default Ports:
  TCP 443, 992 and 5555
  UDP: 1194
- Supported Ciphers:
  AES-128-CBC, AES-192-CBC, AES-256-CBC, BF-CBC, CAST-CBC, CAST5-CBC, DES-CBC, DES-EDE-CBC, DES-EDE3-CBC, DESX-CBC, RC2-40-CBC, RC2-64-CBC and RC2-CBC
- Supported Hashes:
  SHA, SHA1, MD5, MD4 and RMD160
- Operational Mode: L2 (Bridging) and L3 (Routing)
- Compatible VPN Clients: OpenVPN for PC (Windows, Mac, Linux) and OpenVPN Connect by OpenVPN Technologies, Inc.
- Compatible Client OS: Windows, Linux, Mac, iOS and Android
- Supported VPN Topologies: Remote-access VPN, Site-to-Site VPN (L2-Bridging) and Site-to-Site VPN (L3-Routing)

SSTP Server Function Specifications on SoftEther VPN Server

- Clone Function for SSTP-VPN Server of Microsoft's Windows Server 2008 R2 / 2012.
- User-authentication Methods: PAP and MS-CHAPv2
- Supported Ciphers and Hashes on TLS:
  RC4-MD5, RC4-SHA, AES128-SHA, AES256-SHA, DES-CBC-SHA and DES-CBC3-SHA
- Compatible VPN Clients: Built-in VPN Clients on Windows Vista, 7, 8, RT
- Compatible Client OS: Windows Vista, 7, 8, RT, Server 2008, Server 2008 R2, Server 2012
- Supported VPN Topologies: Remote-access VPN

L2TPv3 Server Function Specifications on SoftEther VPN Server

- Clone Function for Cisco's L2TPv3 Site-to-Site VPN Server
- NAT-Traversal: RFC3947 IPsec over UDP Encapsulation

- Transport UDP Ports:
  UDP 500 and 4500
  (Allow both ports on the firewall. Add UDP port forwarding for both 500 & 4500 on the NAT.)
- Supported Ciphers:
  DES-CBC, 3DES-CBC, AES-CBC, Blowfish-CBC and CAST-128-CBC
- Supported Hashes:
  MD5 and SHA-1
- Supported Diffie-Hellman Groups:
  MODP 768 (Group 1), MODP 1024 (Group 2) and MODP 1536 (Group 5)
- Supported VPN Topologies: Site-to-Site VPN (L2-Bridging)
- Compatible VPN Clients: Cisco IOS's L2TPv3 VPN Client
- Compatible Client OS: Cisco IOS or other compatible O

EtherIP Server Function Specifications on SoftEther VPN Server

- NAT-Traversal: RFC3947 IPsec over UDP Encapsulation
- Supported Ciphers:
  DES-CBC, 3DES-CBC, AES-CBC, Blowfish-CBC and CAST-128-CBC
- Transport UDP Ports:
  UDP 500 and 4500
  (Allow both ports on the firewall. Add UDP port forwarding for both 500 & 4500 on the NAT.)
- Supported Hashes:
  MD5 and SHA-1
- Supported Diffie-Hellman Groups:
  MODP 768 (Group 1), MODP 1024 (Group 2) and MODP 1536 (Group 5)
- Supported VPN Topologies: Site-to-Site VPN (L2-Bridging)
- Compatible VPN Clients: EtherIP VPN Client
- Compatible Client OS: EtherIP compatible OS

Requirements

Supported Operating Systems

- **Windows (32bit, 64bit)**
  Windows 98 / 98 SE / ME / NT 4.0 SP6a / 2000 SP4 / XP SP2, SP3 / Server 2003 SP2 / Vista SP1, SP2 / Server 2008 SP1, SP2 / Hyper-V Server 2008 / 7 SP1 / Server 2008 R2 SP1 / Hyper-V Server 2008 R2 / 8 / Server 2012 / Hyper-V Server 2012 / 8.1 / Server 2012 R2 / 10 / Server 2016

- **Linux (32bit, 64bit)**
  Linux 2.4, 2.6, 3.x, 4.x

- **Mac OS X (32bit, 64bit)**
  Mac OS X 10.4 Tiger / 10.5 Leopard / 10.6 Snow Leopard / 10.7 Lion / 10.8 Mountain Lion

- **FreeBSD (32bit, 64bit) (Server and Bridge only)**
  FreeBSD 5, 6, 7, 8, 9

- **Solaris (32bit, 64bit) (Server and Bridge only)**
  Solaris 8, 9, 10, 11

Supported CPUs

- **Windows**
  Intel x86 (32bit), Intel x64 (64bit)

- **Linux**
  Intel x86 (32bit), Intel x64 (64bit), PowerPC (32bit), ARM EABI (32bit), ARM legacy ABI (32bit), MIPS Little-Endian (32bit), SH-4 (32bit)

- **Mac OS X**
  Intel x86 (32bit), Intel x64 (64bit), PowerPC (32bit), PowerPC G5 (64bit)

- **FreeBSD**
  Intel x86 (32bit), Intel x64 (64bit)

- **Solaris**
  Intel x86 (32bit), Intel x64 (64bit), SPARC (32bit), SPARC (64bit)

Hardware Requirements for SoftEther VPN Server

- **Free RAM**
  Minimum: 32Mbytes + 0.5Mbytes * (Number of Concurrent VPN Sessions)
  Recommended: 128Mbytes + 0.5 Mbytes * (Number of Concurrent VPN Sessions)

- **Free Disk Space**
  Minimum: 100Mbytes
  Recommended: 2Gbytes (for daily VPN connection logs)

Hardware Requirements for SoftEther VPN Client

- **Free RAM**
  Minimum: 16Mbytes

Recommended: 32Mbytes

OpenVPN vs. SoftEther VPN

Popular Question: What is the advantage of SoftEther VPN to OpenVPN?

Obviously, OpenVPN is an excellent tool. However, the development of OpenVPN has been stalled for many years. And as you know OpenVPN has no significant improvement in recent years.

The following table will show that the more benefit that SoftEther VPN can provied you. SoftEther VPN supports multi VPN protocols and multi native-VPN clients of various operating systems. SoftEther VPN has an easy-to-use VPN server management GUI tool. SoftEther VPN has also multi-language support. There are any other advantages in SoftEther VPN. Furthermore, SoftEther VPN has the OpenVPN-clone server function. It means that any OpenVPN users can replace it to SoftEther VPN seamlessly.

The SoftEther VPN Project believes that SoftEther VPN has the potential ability to occupy the even stronger position in today's OpenVPN.

comparison3.png