SoftEther VPN
From Wikipedia, the free encyclopedia

SoftEther VPN is a free open-source, cross-platform, multi-protocol VPN solution developed as part of Daiyu Nobori's master's thesis research at the University of Tsukuba. VPN protocols such as SSL VPN, L2TP/IPsec, OpenVPN and Microsoft Secure Socket Tunneling Protocol are provided in a single VPN server. It was released using the GPLv2 license on January 4, 2014.

The architecture of SoftEther VPN was designed for firewall penetration. Support for NAT traversal is provided, making it possible to set up a VPN server behind an organization's or government's firewall. Firewalls performing deep packet inspection are unable to detect SoftEther's VPN transport packets as a VPN tunnel because HTTPS is used to camouflage the connection.

Performance optimization was another objective for SoftEther VPN. It employs strategies such as full Ethernet frame utilization, reducing memory copy operations, parallel transmission, and clustering. Together, these reduce latency normally associated with VPN connections while increasing throughput.

### Contents

- 1 Interoperability
- 2 VPN Server
- 3 VPN Client
- 4 VPN Bridge
- 5 VPN Server Manager for Windows
- 6 VPN Command-Line Admin Utility
- 7 Architecture
  - 7.1 Virtual Hub
  - 7.2 Virtual Network Adapter
  - 7.3 Virtual Layer-3 Switch
  - 7.4 Cascade Connection between Virtual Hubs
  - 7.5 Local Bridge between Virtual Hubs and Physical Ethernet Segment
  - 7.6 Firewall, Proxy and NAT Transparency
  - 7.7 Parallel Transmission Mechanism of Multiple SSL-VPN Tunnels
  - 7.8 NAT Traversal
  - 7.9 VPN over ICMP, and VPN over DNS
  - 7.10 VPN Gate
- 8 See also
- 9 References
- 10 External links

### Interoperability

The VPN Server and VPN Bridge support Windows, Linux, Mac OS X (but not 10.9.x), FreeBSD and Solaris operating systems. SoftEther VPN supports its own VPN protocol but is also compatible with OpenVPN, Microsoft Secure Socket Tunneling Protocol (SSTP), SSL VPN, EtherIP, L2TPv3 and IPsec. Mobile devices running iOS, Android, and Windows Phone are supported via L2TP/IPsec. SoftEther's native VPN Client is supported on Windows, Linux, and Mac. VPN clients and endpoints supporting the other VPN protocols may also be used; this includes a wide variety of routers from companies such as Cisco, Juniper, Linksys (with DD-WRT), Asus, and many others.

### VPN Server
SoftEther VPN Server implements the VPN server function to listens and accepts connections from VPN Client or VPN Bridge with several VPN protocols.

A VPN Server can have several Virtual Hubs and Virtual Layer-3 Switches. A Virtual Hub has full layer-2 Ethernet packet-switching functions like a physical Ethernet switch. Additionally, a Virtual Hub can be configured to define IP packet filter entries to filter the packets through the Virtual Hub. A Virtual Layer-3 Switch has layer-3 IP static routing functions like a physical router.

A VPN Server can have local-bridges. A local bridge is the layer-2 packet-switching fabric between a physical Ethernet network-adapter and a Virtual Hub. The administrator defines a local-bridge between the Virtual Hub and the existing corporate network to build a remote-access VPN server or a site-to-site VPN server.

**VPN Client**

SoftEther VPN Client is a VPN client program which has the virtualized function of an Ethernet network adapter. A computer with installed SoftEther VPN Client can establish a VPN connection to the VPN Server. Since the VPN Server has the support for multiple VPN protocols such as L2TP/IPsec or MS-SSTP VPN, VPN users are not required to install SoftEther VPN Client on client computers. When a user uses L2TP/IPsec or MS-SSTP VPN to connect to the VPN Server, the built-in VPN client programs on the operating system can be used to establish a VPN to the VPN Server. However, SoftEther VPN Client has advanced functions (e.g. more detailed VPN communication settings) than OS built-in VPN clients. To exploit the full performance of SoftEther VPN Server, it is recommended to install SoftEther VPN Client on each client computer.

**VPN Bridge**

SoftEther VPN Bridge is a VPN program for building a site-to-site VPN. To build a site-to-site VPN network, the system administrator has to install SoftEther VPN Server on the central site, and has to install SoftEther VPN Bridge on one or more remote sites. A VPN Bridge connects to the central VPN Server by cascade connection. A cascade connection is similar to, but a virtualized of, an uplink connection (cross-cable connection) between two physical Ethernet switches.

**VPN Server Manager for Windows**

The GUI Tool is the administrative tool for SoftEther VPN Server and SoftEther VPN Bridge. It is a program that runs on both Windows and Linux with WINE. A system administrator installs the GUI Tool on his laptop PC, and makes it connect to the remote VPN Server or VPN Bridge for administration. The connection is made by SSL session, and management commands are transported as RPC over SSL.

**VPN Command-Line Admin Utility**

vpncmd is the CUI administrative tool for SoftEther VPN Server, Client and Bridge. It is a program that runs on consoles of every supported operating systems. When a user is unable to use Windows or Linux with WINE, the user can alternatively use vpncmd to manage the VPN programs. vpncmd is also useful to execute a batch operation, such as creating many users on the Virtual Hub, or creating many Virtual Hubs on the VPN Server.

**Architecture**[^4]

Some parts of the architecture of SoftEther VPN are different from typical traditional IPsec-based VPN systems.

**Virtual Hub**

A Virtual Hub is the software-emulated virtual Ethernet switch. It learns and maintains its own forwarding-database table inside. While traditional physical Ethernet switches implement this function by hardware, SoftEther VPN implements the same function by software. A VPN Server can have several Virtual Hubs. Each Virtual Hub is isolated. A Virtual Hub performs the packet-switching between concurrently connected VPN sessions to realize the communication between VPN Clients and VPN Bridges.
When there are several Virtual Hubs in a single instance of VPN Server, these Virtual Hubs are isolated for security. Each different administrator can have the delegated privilege for each correspondent Virtual Hub. An administrator for a Virtual Hub can define user-objects and ACLs, limited only the delegated Virtual Hub.

**Virtual Network Adapter**

A Virtual Network Adapter is the software-emulated virtual Ethernet adapter. A VPN Client can create several Virtual Network Adapters on the client computer. A VPN user can establish a VPN session between the Virtual Network Adapter and the destination Virtual Hub of the remote VPN Server. While the VPN session is established, the VPN user can communicate to the remote VPN network through the Virtual Network Adapter. Since the Virtual Network Adapter works as if it were the physical one, any applications or operating system components can be used without any modification.

**Virtual Layer-3 Switch**

A Virtual Layer-3 Switch is the software-emulated virtual IP router. Several Virtual Layer-3 Switches can be created on a single VPN Server instance. A Virtual Layer-3 Switch has virtual IP interfaces connected to Virtual Hubs. It also has several static routing table entries.

The Virtual Layer-3 Switch is useful to make a large-scale site-to-site VPN network. Although the easy way to make a site-to-site VPN network is to build the layer-2 bridging based VPN, if the number of computers is huge the number of broadcasting packets will increase to load the inter-site links. To prevent that scaling problem, the VPN administrator isolates IP networks by Virtual Layer-3 switch.

**Cascade Connection between Virtual Hubs**

The administrator can define a cascade connection between local or remote Virtual Hubs. After the cascade connection has been established, the originally-isolated two Ethernet segments are combined to the single Ethernet segment. Therefore, the cascade connection function is used to build the site-to-site layer-2 Ethernet bridging.

**Local Bridge between Virtual Hubs and Physical Ethernet Segment**

Since Virtual Hubs and Virtual Network Adapters are only software-emulated virtual Ethernet devices, the Ethernet packets through these virtual devices cannot communicate with physical Ethernet devices. Therefore, a bridge between the virtual and the physical is necessary to build a remote-access VPN or site-to-site VPN. To make a bridge, the Local Bridge function exchanges the Ethernet packets between a Virtual Hub and a physical Ethernet network adapter to combine both isolated Ethernet segments into a single Ethernet segment.

After defining the Local Bridge on SoftEther VPN Server, any VPN Client can connect to the VPN Server and communicate to all existing Ethernet devices (e.g. servers or network equipment) through the Local Bridge. This is called a remote-access VPN.

If the network administrator sets up the remote-site VPN Bridge, and defines two Local Bridges on both VPN Server and VPN Bridge, and defines a cascade connection between VPN Server and VPN Bridge, then the remote two Ethernet segments are connected directly in layer-2 Ethernet level. This is called a site-to-site VPN.

**Firewall, Proxy and NAT Transparency**

One of the key features of SoftEther VPN is the transparency for firewalls, proxy servers and NATs (Network Address Translators). To do this, SoftEther VPN supports SSL-VPN and NAT Traversal. SoftEther VPN uses HTTPS protocol in order to establish a VPN tunnel. HTTPS (HTTP over SSL) protocol uses the TCP/IP port 443 (may vary) as destination.

**Parallel Transmission Mechanism of Multiple SSL-VPN Tunnels**

When the user chooses SSL-VPN protocol between the VPN Client and VPN Server, SoftEther VPN Server and VPN Client use a parallel transmission mechanism to improve the throughput of the SSL-VPN tunnel. A user can set up the number of concurrent parallel transmission channels from 1 to 32. In an environment such as a slow and delaying network, this performance tuning will result in a faster throughput. When this function is enabled, the logical VPN
Session will consist of several TCP (HTTPS) connections. All packets will be added to one of the appropriate TCP connections with calculations of optimizing modules. If some packet losses have been detected on a TCP connection of the logical VPN Session, then the new packet will use another healthy VPN connection. This fast-switching optimization to determine the processing TCP connection enables high throughput.

NAT Traversal

Traditional VPN systems require the user to ask the firewall's administrator of the company to open an endpoint (TCP or UDP port) on the firewall or NAT on the border between the company and the Internet. In order to reduce the necessity to open an endpoint on the firewall, SoftEther VPN Server has the NAT Traversal function. NAT Traversal is enabled by default. As long as it is enabled, SoftEther VPN Client computers can connect to your VPN Server behind the firewall or NAT. No special settings on the firewall or NAT are necessary.

VPN over ICMP, and VPN over DNS

A few very-restricted networks only permit to pass ICMP or DNS packets. On such a network, TCP or UDP are filtered. Only ICMP and DNS are permitted. In order to make it possible to establish a SoftEther VPN client-server session via such a very-restricted network, SoftEther VPN has the "VPN over ICMP" and the "VPN over DNS" function.

This function is very powerful to penetrate such a restricted firewall. All VPN packets are capsuled into ICMP or DNS packets to transmit over the firewall. The receiver-side endpoint extracts the inner packet from the capsuled packet. This is very useful for exploiting public Wi-Fi. Some public Wi-Fi can pass only ICMP or DNS packets. They filter TCP or UDP packets. If you have a VPN Server installed on your home or office in advance to go outdoor, you can enjoy protocol-free network communication by using such a restricted network.

VPN Gate

VPN Gate is a plugin for SoftEther VPN, which allows users to connect to free VPN servers, run by volunteers who use SoftEther to host their VPN servers. VPN Gate is sponsored by the University of Tsukuba. [5][6]

See also

- OpenVPN, an open-source VPN program
- UDP hole punching, a technique for establishing UDP "connections" between firewalled/NATed network nodes
- Secure Socket Tunneling Protocol (SSTP) Microsoft method for implementing PPP over SSL VPN

References

1. Authors of SoftEther VPN on GitHub (https://github.com/SoftEtherVPN/SoftEtherVPN/blob/master/AUTHORS.TXT)
3. License of SoftEther VPN (http://www.softether.org/4-docs/1-manual/1_SoftEther_VPN_Overview#1.3_SoftEther_VPN_is_Freeware)
4. Layer-2 Ethernet-based VPN (http://www.softether.org/1-features/2_Layer-2_Ethernet-based_VPN)

External links

- SoftEther VPN Project web site (http://www.softether.org/)
- SoftEther VPN Users Forum (http://www.vpnusers.com/)
- Create SoftEther VPN Account Online (https://www.fastssh.com/page/softether-servers)
- Multi-protocol SoftEther VPN becomes open source (http://www.net-security.org/secworld.php?id=16171) (by net-security.org)