1. Ultimate Powerful VPN Connectivity

1.1. 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). NATs are sometimes implemented on broadband router products.

1.1.1.jpg

Only HTTP/HTTPS traffics can pass through the restricted firewall. SoftEther VPN is based on HTTPS.

Backgrounds

Generally, in company networks of nowadays, there are firewalls to isolate between the inside network and outside for ensuring security. Not only for purpose of security, but also companies use firewalls, proxies and NATs in order to share the precious IP addresses with many computer users in the office. So such devices are indispensable today.

Tunnels of legacy VPN protocols, such as IPsec, L2TP and PPTP, cannot often be established through firewalls, proxy servers and NATs. There protocols were developed in the era before NATs were widely spread. For example, IPsec and L2TP use ESP (Encapsulating Security Payload) packets, and PPTP uses GRE (Generic Routing Encapsulation) packets. These packets are special forms of IP packets. Therefore generally firewalls, proxies and NATs are unable to pass these legacy VPN packets. Recently some venders of VPN products with IPsec, L2TP and PPTP tried to invent the extend method to pass through these wall devices, and some of VPN products are implemented with that extensions. But such extensions of legacy VPN protocols still have a problem of compatibles. In many cases, a user tries to establish a VPN connection by either L2TP or PPTP on the network which is with firewalls, proxy servers and NATs, but he will fail. You might have an experience that you stayed in the hotel room and tried to connect to your company's network by remote access VPN with either L2TP or PPTP but failed. The reason why it failed is that firewalls, proxy servers and NATs on the network were incompatible with either L2TP or PPTP.

Hence, it can be said that today's network administrators have a headache for a problem of incompatibles between VPN connections and security devices.

SoftEther VPN's Solution: Using HTTPS Protocol to Establish VPN Tunnels

SoftEther VPN uses HTTPS protocol in order to establish a VPN tunnel. HTTPS (HTTP over SSL) protocol uses the 443 of TCP/IP port as destination. This port is well-know and almost all firewalls, proxy servers and NATs can pass the packet which are consisted in HTTPS protocol.

1.1.2.jpg

Unlike legacy VPNs, SoftEther VPN adopts "Ethernet over HTTPS" encapsulation.

HTTPS protocol is widely used on the Internet. When you open a web browser and access to the web site with security communications, HTTPS is used automatically. Thanks to HTTPS, you can transmit secret information such as credit card numbers via the Internet. Today's society activities are depending on HTTPS. Without HTTPS, you can no longer to use the Internet as a tool for electrical commercial transactions.

Due to the fact that HTTPS is de-facto standard, almost all firewalls, proxy servers and NATs opens a path for HTTPS. Anyone who is in the LAN (Local Area Network) can establish any HTTPS connection between their hosts and any hosts on the Internet remotely. Exploiting this condition is the best way to realize a good transparency for VPN protocol.

Thus, SoftEther VPN adopted HTTPS as the protocol for stabilizing and tunneling mechanism for VPN. SoftEther VPN can be used within almost all network environments, such as enterprise LAN, hotel room and airport free Wi-Fi access, differ to any other legacy VPNs such as IPsec, PPTP and L2TP.

Due to this feature of SoftEther VPN, you can easily design your own VPN topology which is suitable for your demands with a minimal effort of modifying the existing current your network security devices. If you want to use SoftEther VPN on your network, you need few efforts of modifying the current configuration and policy on your network thanks to SoftEther VPN's feature of good connectivity.

On the other hand, if you want to use legacy VPNs on your network, you have to modify the current network policies on the security devices such as firewall to allow passing the special IP protocol such as ESP and GRE. You also have to modify the configuration file on the firewall. Such works needs your extra effort and might cause some troublesome side effects on your stable and precious network. Not only bothering you by requirements of your efforts, you will have a risk to make the network dangerous because you have to change the setting of the firewall to punch a hold on it in order to allow passing the packet of legacy VPNs. If you use SoftEther VPN, you don't need either of these efforts and risks.

Some networks such as airport Wi-Fi and hotel-room Internets are restricting of using any other VPN else HTTP and HTTPS, due to security reason. In such a highly restricted network, the only single way to use VPN is to use HTTPS-packet-tunneling VPN such as SoftEther VPN.

Conclusions: SoftEther VPN is not just a VPN, but also very good VPN for an aspect of compatibility for Firewalls, Proxies and NATs.

1.2. Supports Multiple Standard VPN Protocols

SoftEther VPN Server supports not only VPN over HTTPS protocol described in the section 1.1. SoftEther VPN Server supports also L2TP/IPsec, OpenVPN, MS-SSTP, L2TPv3 and EtherIP protocols. They are Internet VPN standard protocols.

Your iPhone, iPad, Android, Windows Mobile and other mobile devices are now able to connect to your SoftEther VPN Server from anywhere, anytime. You can also use Cisco Systems or other VPN router vendor's edge VPN products which are supporting L2TPv3/IPsec or EtherIP/IPsec in order to connect to your SoftEther VPN Server.

1.2.jpg

SoftEther VPN Server supports traditional VPN protocols as above.

Support L2TP/IPsec Protocol

The following devices have built-in L2TP/IPsec VPN clients. They can connect to your SoftEther VPN Server, without any installation of client software on such devices.

iphone.jpg

Your Mac, iPhone, iPad or Android can connect to SoftEther VPN Server.

- iPhone
- iPad
- Android
- Windows Mobile
- Windows XP / Vista / 7 / 8 / RT
- Mac OS X

IMG_4091.PNG

iPhone and Android can connect to SoftEther VPN Server.

ss1.2_2.jpg

L2TP/IPsec Configuration is very easy with GUI.

Support OpenVPN Protocol

SoftEther VPN Server has a "clone function" of OpenVPN. If you have already installed OpenVPN for remote-access VPN or site-to-site VPN, you can replace the current OpenVPN Server program to SoftEther VPN Server program, and you can enjoy the strong functions and high-performance abilities of SoftEther VPN.

The "close function" of OpenVPN on SoftEther VPN Server works same to OpenVPN Technologies, Inc.'s implementation, not only enough but also better performance and functionality. Your OpenVPN Client devices or edge-sites of VPN can connect to new SoftEther VPN Server very easily. You can adopt SoftEther VPN on both remote-access L3 VPN and site-to-site L2 VPN.

The advantages to adopt SoftEther VPN Server instead of old OpenVPN Server program are as follows:

- SoftEther VPN Server has easier configuration than OpenVPN Server by OpenVPN Technologies, Inc.
- You can use Automated OpenVPN Configuration File Generator tool to make a configuration file (.ovpn) for VPN client.
- SoftEther VPN Server supports not only OpenVPN. It supports all standard VPN functions, including SSL-VPN, L2TP/IPsec, MS-SSTP, L2TPv3/IPsec and EtherIP/IPsec. So you can integrate OpenVPN and other protocol's VPN servers into just one VPN Server by using SoftEther VPN Server.
- User administration and security settings can be configured by GUI tools. The management functions are integrated. You can use single-path operation to manage the server.
- All operating system which supports OpenVPN (e.g. Linux, Mac OS X, Linux, UNIX, iPhone and Android) can connect to SoftEther VPN Server.

ss1.2.jpg

You can activate OpenVPN easily with GUI.

IMG_4099.PNG

Not only PC-version OpenVPN. You can also use OpenVPN Client on iPhone / Android.

Support Microsoft SSTP VPN Protocol

SoftEther VPN Server has a "clone function" of Microsoft SSTP VPN Server. You can connect to SoftEther VPN Server from Windows 7 / 8 / RT with built-in SSTP VPN Clients. SSTP (Secure Socket Tunneling Protocol) is a PPP over HTTPS protocol which Microsoft Corporation suggested.

Originally, SSTP VPN Server functions are implemented on only Microsoft Windows Server 2008 / 2012. However, licensing fees of such Microsoft's server operating systems are very expensive. They are also difficult to configure for normal-skilled users. You can use SoftEther VPN Server to realize almost same functions and performances by using the close server of Microsoft SSTP VPN Server.

The advantages to adopt SoftEther VPN Server instead of Microsoft SSTP VPN Server are as follows:

- Very easy configuration than Microsoft's SSTP VPN Server.
- No need to install a VPN Client on Windows clients. Built-in SSTP VPN client on Windows can be used to connect to SoftEther VPN Server.
- Windows RT (ARM version of Windows) also has a built-in SSTP VPN client.
- User administration and security settings can be configured by GUI tools. The management functions are integrated. You can use single-path operation to manage the server.
- You are no longer to need purchase expensive Windows Serer 2008 / 2012. It can save your cost.
- The SSTP VPN Server Clone Function of SoftEther VPN Server runs on non-Windows operating systems. It works on Linux, Mac OS X, FreeBSD and Solaris perfectly.

Support L2TPv3/IPsec and EtherIP/IPsec Protocols

Most of Cisco System's router products and other vendor's products supports L2TPv3/ IPsec or EtherIP/IPsec VPN protocols. These protocols are to make site-to-site L2 bridging VPNs. SoftEther VPN Server supports L2TPv3 and EtherIP over IPsec. You can build a site-to-site L2 bridge connection by using your Cisco's router as an edge, and SoftEther VPN Server as a center. This has an advantage to reduce the cost. Cisco's center routers are very expensive. You can simply replace Cisco's high-end router in the center of VPN, to SoftEther VPN Server.

1.3. Faster than Microsoft's and OpenVPN's implementation

We have **conducted the performance test** at a laboratory at Graduated School of Computer Science at University of Tsukuba in the end of 2012.

We had 5 protocols to test: SoftEther VPN, L2TP/IPsec, SSTP, OpenVPN (Layer-3 mode) and OpenVPN (Layer-2 mode). We tested both our SoftEther VPN Server implementation and existing implementation by Microsoft Corporation or OpenVPN Technologies, Inc. to evaluate SoftEther VPN's performance. The testing environment was: Windows Server 2008 R2 x64 on Intel Xeon E3-1230 3.2GHz and Intel 10 Gigabit CX4 Dual Port Server Adapter.

- SoftEther VPN Protocol achieved **980Mbps** by using SoftEther VPN Server.
- L2TP/IPsec Protocol resulted **614Mbps** by SoftEther VPN Server, while resulted **593Mbps** by Microsoft's Windows Server 2008 R2's Routing and Remote Access service (RRAS).
- SSTP resulted **737Mbps** by SoftEther VPN Server, while resulted **715Mbps** by Microsoft' s Windows Server 2008 R2.

- OpenVPN (L3) resulted **89Mbps** by SoftEther VPN Server, while resulted **76Mbps** by OpenVPN's original implementation.
- OpenVPN (L2) resulted **90Mbps** by SoftEther VPN Server, while resulted **83Mbps** by OpenVPN's original implementation.

As the results, SoftEther VPN Server was faster **103.5%** than Microsoft's Windows implementation in L2TP/IPsec, faster **103.0%** than Microsoft's Windows implementation in SSTP, and faster **108-117%** than OpenVPN's original implementation. Moreover, our SoftEther VPN Protocol (Ethernet over HTTPS, described at the section 1.1) resulted **980Mbps**, which is faster **159.6%** faster than L2TP/IPsec Protocol, **175.2%** faster than SSTP Protocol and **x9.8 times** faster than OpenVPN Protocol.

This result proves SoftEther VPN Server as the fastest VPN server program in the world.

- **More details are here.**

1.4. Built-in Dynamic DNS (*.softether.net)

Most of all existing VPN solutions need a fixed global IP address for stability. Fixed global IP addresses need monthly costs to pay to ISPs. And global IP address shortage is now serious problem of our world.

SoftEther VPN has a built-in Dynamic DNS (DDNS) function to mitigate the above problems. Dynamic DNS function is enabled by default. DDNS function registers your

VPN Server's IP address on the DNS record of ".softether.net" , which is the domain-suffix operated by SoftEther Corporation and University of Tsukuba, for free of charge.

A DDNS FQDN "abc.softether.net" (the "abc" part is the identifier that a user can specify) will be assigned to your SoftEther VPN Server. You can tell the DDNS hostname to your VPN Server's users. A user of your VPN Server can now specify the DDNS hostname as a destination. If the corresponding IP address will be changed in future suddenly, the registered IP address of the DDNS hostname will follow the new IP. This mechanism makes fixed global IP addresses no longer necessary, and you can reduce the cost to pay ISPs monthly.

1.4.jpg

Dynamic DNS is natively supported by SoftEther VPN.

ss1.4.jpg

The Dynamic DNS function easy-setup screen.

1.5. NAT Traversal

By using existing VPN systems, you need to ask the firewall's administrator of your company to open an endpoint (TCP or UDP port) on the firewall / 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. During it is enabled, SoftEther VPN Client computers can connect to your VPN Server behind the firewall / NAT. No special settings on the firewall / NAT are necessary.

You can disable the NAT Traversal function on your VPN Server by switching the value of "DisableNatTraversal" to "true" in the VPN Server's configuration file. You can also disable it by appending the "/tcp" suffix on the destination hostname.

1.5.jpg

NAT Traversal function penetrates your office's firewall.

1.6. VPN over ICMP, and VPN over DNS (Awesome!)

A few very-restricted networks only permit to pass ICMP or DNS packets. We don't know the reason. On such a network, TCP or UDP are filtered. Only ICMP and DNS are transferred.

In order to make it possible to establish 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 over ICMP, and VPN over DNS are implemented based on ICMP and DNS protocol specifications. However, they sometimes behaves irregularly. It might causes

memory-overflow or something problems on the "buggy routers" on the network. Some routers might reboot because of these problems. It might affect other users of Wi-fi around you. In such an event, disable VPN over ICMP and VPN over DNS functions by appending "/tcp" suffix after the destination hostname.

1.6.jpg

Your payload traffics will be divided and encapsulated into ICMP packets. Awesome!

ss1.6.jpg

You can activate both VPN over ICMP and VPN over DNS with a simple step.

1.7. VPN Azure Cloud Service (Academic Experiment)

If your SoftEther VPN Server is behind the firewall or NAT, and if all of NAT Traversal, Dynamic DNS and VPN over ICMP/DNS functions failed to work well, do not give up. You can use "VPN Azure Cloud Service" as the final trump.

All existing VPN systems need to ask the firewall's administrator to open some TCP or UDP ports. And at least one fixed global IP address is required on the network. They are very inconvenient.

To solve the existing problems, we introduce the "VPN Azure Cloud Service" . This service is provided by SoftEther Corporation and University of Tsukuba as an academic experiment. You can connect to your VPN Server behind the firewall from other VPN clients on the remote side, without opening any TCP/UDP ports on the firewall, if you have activated the VPN Azure function on the VPN Server in advance. The VPN Server

will connect a TCP connection "from inside to outside over the firewall" . The connection will be kept towards a relaying server on the VPN Azure Cloud Servers. You can connect to a relaying point on a cloud server from a VPN Client. The cloud server will relay your all traffics to the destination VPN Server behind the firewall. Once the connection has been made, you can now access to any computers on your company or home network which are protected by the firewall.

Once a VPN Server connects to the VPN Azure Cloud, the server will have a unique hostname "abc.vpnazure.com" ("abc" is unique idenfitier). The hostname is assigned on the appropriate VPN relaying server on the VPN Azure Cloud Service.

VPN Azure Cloud Service function is disabled by default. You can easily activate it on the manager GUI of VPN Server. For details to use, please refer **http://www.vpnazure.net/**.

1.7.jpg

VPN Azure Cloud Service is a free-of-charge powerful VPN-traffic relaying service to penetrate firewalls.

1.8. Works on Many OS and CPUs

SoftEther VPN can work with following operating systems. Other VPN products are strictly bound to some specific systems. For example, Cisco IOS software can work only on Cisco Router hardware which is exclusively sold from Cisco Systems. SoftEther VPN is different. It can be work on not only several operating systems, but also several CPU architectures as follows.

This advantage means that for example if you currently run SoftEther VPN Server on the particular platform, but you want to change the underlying platform, you can change it at

any time. All configuration commands and state files are exactly same between several platforms, because SoftEther VPN software codes were written by C language with very careful effort to keep compatibility and portability between on different systems.

- **Windows**
  Windows 98, 98 SE, ME, NT 4.0, 2000, XP, Server 2003, Vista, Server 2008, 7, Server 2008 R2, 8 and Server 2012 are supported on both Intel x86 (32 bit) and x64 (64 bit, as known as AMD64) platforms by SoftEther VPN Server, Client and Bridge.

- **Linux**
  Linux Kernel 2.4, 2.6 and 3.x are supported on Intel x86 (32 bit), x64 (64 bit), ARM, MIPS and PowerPC platforms by SoftEther VPN Server, Client and Bridge.

- **FreeBSD**
  FreeBSD 5.x, 6.x, 7.x, 8.x and 9.x are supported on Intel x86 (32 bit) and x64 (64 bit) platforms by SoftEther VPN Server and Bridge.

- **Solaris**
  Solaris 8, 9, 10 and 11 are supported on Intel x86 (32 bit), Intel x64 (64 bit), SPARC (both 32 bit and 64 bit) platforms by SoftEther VPN Server and Bridge.

- **Mac OS X**
  Mac OS X 10.4, 10.5, 10.6, 10.7 and 10.8 are supported on Intel x86 (32 bit), Intel x64 (64 bit), PowerPC (32 bit) and PowerPC G5 (64 bit) platforms by SoftEther VPN Server and Bridge.

1.8.jpg

In SoftEther VPN programs, the OS independent modules helps to build a platform-independent VPN server.