1.1 What is SoftEther VPN?

SoftEther VPN is next-generation VPN software that offers stability, flexibility and expandability, and is compatible with all advanced networks that produce wide bandwidth an high load required by large corporations and Internet providers as well as networks for individuals and homes and networks for small and medium size businesses.

This section contains an overview of SoftEther VPN, a comparison with older VPN protocol, and a description of its advanced functions.

1.1.1 History

SoftEther VPN was previously developed and distributed as "SoftEther 1.0". SoftEther (old) was developed by Daiyuu Nobori, a student of University of Tsukuba, as a personal project. "SoftEther" was software that enabled users to construct a simple layer 2 VPN by installing a Virtual Network Adapter and Virtual Ethernet Switching Hub on Windows, and was distributed as freeware. "SoftEther" later became a project of the research and development project of Japanese Government, subsidized by Ministry of Economy, Trade and Industry of Japan, administrated by Information Promotion Agency, in 2003.

SoftEther VPN (the subject of this manual) is VPN software that is the next version of "SoftEther". SoftEther VPN is now developed and released as "freeware", from the SoftEther Project at University of Tsukuba, Japan. SoftEther VPN is planned to become open-source software in middle of 2013.

1.1.2 Structure and Operating Principle of VPN

Virtual Private Network (VPN) is a technology that started to spread around 1998. VPN technology allows users to construct a virtual network that maintains security in an existing IP network such as the Internet and communicate freely within the virtual network.

The following is a description of common VPN structure.

Tunneling and Encapsulating

VPN is a solution for constructing a virtual network. A technique called "tunneling" that enables users to construct a virtual network between two remote points on an existing public IP network and communicate freely is used in the VPN.

With tunneling technology, packets transmitted on a physical communications medium such as conventional network cable or optical fiber are encapsulated as data of another protocol such as TCP/IP packets without directly transmitting on a physical network.

Encryption and electronic signature can be added simultaneously when encapsulating. Encapsulated data is transmitted through a session called a "tunnel" between the start and end point of VPN communication. The other party who receives the encapsulated data removes the original packets from the capsules. If the data is encrypted when encapsulated, it must be decrypted. If an electronic signature has been added, the user can check whether the contents of the packet have been tampered with during transmission by testing the integrity of the electronic signature.

When VPN communication is to be carried out, because the data transmitted between the computer sending the data and the computer receiving the data travels through the tunnel is sent encapsulated, unprotected data is never exposed on the network.

1-1-2.png

Structure and operating principle of common VPN.

Ensuring Security of Transmitted Data by Encryption

One of the advantages of using VPN is enhanced security by encryption.

An IP network that can be accessed by anyone such as the Internet is always exposed to danger of eavesdropping and masquerading. Even if expensive transmission services and infrastructure such as dedicated line service or satellite links are used, the lines could be physically bugged or data could be surreptitiously viewed by communications company technicians maliciously or out of curiosity, or could be tapped and analyzed by the government, etc. When sending and receiving data over such WAN, it is therefore recommended that data by encrypted by some means.

1-1-3.png

Danger of sending and receiving data over the Internet.

The fact is that not all existing communication applications and protocols support encryption is a possible problem. For example, HTTP protocol includes a protocol called HTTPS which is encrypted by SSL. And this SSH protocol is encrypted from the

beginning. Numerous Internet based applications however either do not have an encryption function, or if they do, they might have a problem with packaging or encryption strength.

1-1-4.png

Encrypted packets and packets that are not encrypted.

If using these conventional communications protocols with insufficient security as they are on WAN such as dedicated lines or the Internet, the data can be intercepted or altered by hacking.

Security can be dramatically enhanced by automatically encrypting communication of almost all applications using IP or Ethernet by utilizing VPN.

Better Connectivity and Network Independence

Another significant advantage of using VPN is that it enhances connectivity and offers network independence.

Because with the public IP networks such as the Internet, as a rule, any IP packet can be transmitted from a computer of any IP address to another computer of any IP address. If data is to be transmitted over the Internet, when communication is to be conducted between a client computer and server computer, the server computer may actually receive packets from a different computer with malicious intent. Nowadays vulnerable operating systems and worms that open security holes in transmission software and server software on the Internet are going around and there is a possibility of infection. Because the computer which directly connected to the Internet is substantially unsafe, it is not

recommended that computers that process important communications data for business, etc., be allotted direct Internet global IP addresses and connected to the Internet.

However when sending and receiving data between remote bases via public IP network such as the Internet, as a rule, at least one global IP address port must be open and standing by for communications. This is necessary along with using TCP/IP protocol. Thus when sending and receiving data between computers at remote bases if VPN is not used attainability, it must be secured for IP packets of both computers in which case problems may occur with that has mentioned in security earlier.

1-1-5.png

When carrying out TCP/IP connection on the Internet as a rule
at least one must have a global IP address and the port must be open to the public.

By using VPN these problems can be easily and reliably solved. In the fact that VPN carries out communication with the structure whereby encapsulated packets flowing in the tunnel established between computers at remote bases as it was mentioned earlier when establishing the tunnel, user authentication is mutually conducted between the computers and the tunnel is established only if successful. Also once the tunnel is established, as long as physical network communication is not cut off, it is constantly maintained and all the data flowing through the tunnel is encrypted. And if electronic signature is added, other computers on the Internet which is not related to the tunnel can no longer interrupt communications of that tunnel.

Using this tunnelling technology, multiple computers and LANs deployed in several remote locations can be securely connected together over the avaialbe, insecure, WAN and Internet.

1-1-6.png

Prevention of eavesdropping/tampering by third party with malicious intent using VPN.

Inexpensive Internet Connection can be Used Instead of Dedicated Line

By utilizing the structure of VPN such as previously described, without using dedicated line services that is used to charge high usage fees, with more robust security that dedicated line services, communications can be conducted between computers of any base via the Internet.

Especially recently, for several thousand yen per month, because Internet services using optical fiber or ADSL are available, such inexpensive services can be used for same or safer communications purpose.

By using VPN, public networks whereby any computers can communicate freely by IP Internet. It can establish a company dedicated virtual communications network within that network, and a safe and stable independent network that can be constructed without worrying about danger of Internet.

1-1-7.png

Using inexpensive and fast Internet connection instead of dedicated line.

1.1.3 Limitations of old VPN Solution

Several VPN software and hardware solutions have existed for some time, and since 1998 VPN technology and technologies employing it has been used at various sites. For example the following VPN protocols are currently incorporated into several network products and has been used.

- PPTP
- L2TP / IPSec
- vtun
- OpenVPN
- Port transmission by SSH
- Other minor VPN standards

However many older VPN protocols have the following limitations, and under various circumstances, uses must be restricted or cannot be used.

Difficulty of Pass of Network Gateway Devices

Many home and business private networks are separated from the Internet by a network gateway device such as a NAT (IP masquerading), proxy servers and firewalls. These gateway devices may be a dedicated device (appliance) or a high performance computer running Linux etc. The gateway device performs both security functions as well as limiting the number of actual Internet addresses needed to connect the private network to the Internet.

However many older VPN protocols cannot communicate via this network gateway device. One reason for this is many VPN protocols use special headers when encapsulating communications packets that are not part of ordinary TCP/IP protocol. For example a VPN protocol called PPTP uses an extremely minor protocol called Generic Routing Encapsulation (GRE). A VPN protocol called L2TP furthermore requires use of IPSec, whereby a header is added because it is an IPSec packet.

The result of using non-standard TCP/IP such as mentioned in the examples is that traditional VPN communications are prevented by, or at least impose the need for configuration changes to, most network gateway devices (NAT, proxy server, firewalls). In may also become necessary to allocate global IP addresses to each end of the VPN connection.

1-1-8.png

Many older VPN protocols have difficulty passing NAT router firewalls, etc.

Limitations of Protocol that can Communicate within VPN

Many conventional VPN protocols are limited to layer 3 protocol (IP layer, etc) and furthermore upper layer protocol (TCP layer, application layer, etc.) and communication is conducted by encapsulated tunneling. With this system however VPN protocol cannot be made to individually communicate via VPN with protocols that do not comply.

For example in many cases legacy protocols such as special protocol for control, IPX/SPX and NetBEUI currently used by general purpose equipment cannot be used via VPN and it is difficult to transmit existing system communications using Internet VPN instead of a dedicated line.

1-1-9.png

VPN protocol that encapsulates older IP cannot send and receive packets other than IP packets.

IP Routing is Necessary

Of older VPN protocols, if VPN is realized using types of protocols that encapsulate layer 3 (IP layer), basically one of the following must be selected.

1. Install VPN client software on all computers participating in VPN and connect.
2. Connect existing network of base to VPN and conduct IP routing.

If constructing VPN by method 1, if installing VPN client software on all computers that might be connected to VPN and carrying out VPN communications, by conducting connection operation for the VPN server, communications can be freely carried out only between computers installed with VPN client software. With this method however the more computers there are that want to carry out VPN communications the more administration is necessary, computers for which VPN client software cannot be installed or devices for networks such as other network appliances or digital electrical appliances cannot participate in VPN.

If VPN is constructed by method 2, computers in the network of the base connected to VPN can send and receive data to/from each other, and computers for which VPN client software cannot be installed and devices for networks such as other network appliances and digital electrical appliances automatically participate in VPN. This method is however disadvantageous in that it requires IP routing between existing networks connected to VPN and virtual networks by VPN.

Therefore if remote access VPN or VPN connected between bases is realized by old VPN protocol, it requires large scale setting modification for existing networks such as routing table setting modification for existing IP network routers, etc.

1-1-10.png

Devices that do not support routing cannot communicate via VPN of old IP base.

Dependence on Certain Platform

For many old VPN protocols there is a problem if the range of platforms that support the various VPN protocols is not very wide, and even if they can be used among multiple platforms, differences in respective implementation have caused resulted the trouble in practical application in some cases.

Some VPN protocols furthermore require hardware of certain network device vendors and compatibility of protocols among vendors which declined.

1-1-11.png

Communication among VPN products of different vendors cannot be carried out.

High Cost, Low Performance

Price of network devices and security software is generally extremely high, including network security solutions other than VPN solutions. Realistically however network security products introduced at high cost often do not satisfy performance and function requirements.

Particularly concerning function and performance, the most important factor of conventional VPN is providing security; network permeability and communications performance are not considered as important. The reason for this is, when old VPN protocol began to appear, broadband was not yet very popular but was the fastest Internet connection line available for average businesses and homes whereby speed increased from several Mbps to tens of Mbps.

Currently, even for ordinary homes, with the backbone of broadband line businesses of several tens to 100Mbps, Internet connection lines of gigabit scale are available at an extremely low price compared to several years ago. There is not that much VPN hardware and VPN products that can use these fast physical lines efficiently enough, and even the ones that dose exist are mostly installed on extremely expensive network dedicated devices.

Need for new VPN System to Compensate for Shortcomings in old VPN Protocol

Old VPN protocol includes the problems described above and various other problems. So a high function, reliable, highly flexible VPN system that can solves the problems and limitations was therefore very necessary.

1.1.4 SoftEther VPN's Advantage and Characteristics

Along with solving the various previously limitations of old VPN solutions, SoftEther VPN is the VPN software that many have been waiting for, incorporating many new and innovative functions.

Features of SoftEther VPN

The great advantage of SoftEther VPN is that it overcomes the limitations of older VPN solutions very simply.

SoftEther VPN carries out encapsulation and tunnelling at layer 2, in other words Ethernet. When SoftEther VPN is used, network devices such as conventional network adapters switching HUB and layer 3 switching are realized by software. Using SoftEther VPN, the user creates a highly flexible, secure tunnel based on the widely available and easy TCP/IP protocol.

The operation principle of SoftEther VPN and specifications are explained by 1.4 VPN Processing Principle and Communication Method. The method of actually designing/ constructing and applying various networks by SoftEther VPN is also explained in 10. Examples of Building VPN Networks.

1-1-12.png

Making various types of hardware devices on Ethernet virtual for SoftEther VPN.

Advantages of Making Ethernet Virtual

Unlike the many old VPN protocols, SoftEther VPN targets the layer 2 (Ethernet) for VPN communications. In other words, with VPN which have targeted old layer 3, encapsulated IP packets flowed through the tunnel. But with SoftEther VPN, it will encapsulated Ethernet packets flow though the tunnel.

1-1-13.png

Comparison of old VPN protocol and SoftEther VPN when base-to-base connection VPN is constructed.

1.1.5 NAT, Proxy Server and Firewall Traversal

SoftEther VPN conducts VPN communications by establishing a VPN session called a tunnel between VPN Server and VPN Client or VPN Bridge.

Packets that virtually flow in VPN session which is an Ethernet network are actually encapsulated and flow through a physical IP network. At this point, however, SoftEther VPN encapsulates random Ethernet frames to TCP/IP protocol. This point is a feature that was not present in the majority of old VPN protocols.

Also with SoftEther VPN, any TCP/IP port number can be designated and used for VPN communications. The default port numbers are 5555, 443 (for HTTPS) and 992. For details concerning TCP/IP port number designation, see 3.3 VPN Server Administration.

By conducting all VPN communication by TCP/IP, SoftEther VPN can conduct VPN communication via the majority of network gateway devices. VPN can be easily established through almost all types of NAT proxy servers and firewalls.

When SoftEther VPN is used, VPN communications can be easily and safely conducted proxy server and firewall settings even in environments that used to be hard to use VPN because of NAT.

Because it is no longer necessary to open a hole in existing firewall settings to introduce VPN, the burden on the network administrator is reduced and it helps prevent deterioration of network security due to firewall setting modifications.

Users can also safely access company LAN via free Internet connection spots, such as destination stations and airport hotels when they take along a laptop computer installed with VPN Client. Because many free Internet connection spots have introduced NAT or firewall transparent proxy servers, VPN protocol could not be used in many cases before. however they can be used without worry by equipping the SoftEther VPN.

1-1-14.png

Passage through NAT proxy server or firewall by SoftEther VPN.

1.1.6 Stability and Security

As it was previously mentioned, SoftEther VPN uses TCP/IP protocol only for VPN communications and any Ethernet frames can be tunneled. When VPN communication is carried out, SoftEther VPN encrypts all data by Internet standard encryption protocol which is called Secure Socket Layer (SSL). At this time the system administrator can use any encryption algorithm of electronic signature algorithm administrator chooses. For details see 3.3 VPN Server Administration.

With SoftEther VPN, its not only communications encrypted, but security concerning user authentication and server authentication are bolstered. SoftEther VPN supports user authentication by using the RADIUS servers used by companies, NT domain / Active Directory and certificate authentication using X509 and RSA. Also supports some smart cards used for purposes which is deemed necessary for high security. For details see 1.5 Strong Security Features.

Protocol that has been used for transmitting VPN communications packets and security checks such as user authentication actually flowing through a physical IP network during VPN communications is called SoftEther VPN protocol. SoftEther VPN protocol is not only encrypts all communication contents by SSL, but it establishes several simultaneous SSL connections established between VPN Server and VPN Client or with VPN Bridge. Also by altering the timing by a certain interval and reconnecting, it is able to stably communicate through some special network devices whereby TCP/IP connection which is lost for a certain time interval. Stable VPN communication can also be carried out with telephone lines with high packet loss rate, some ADSL, PHS, wireless LAN, etc. For details see 4.4 Making Connection to VPN Server.

1-1-15.png

User authentication by SoftEther VPN protocol.

1.1.7 High-speed Communications Throughput

Many older VPN protocols focused only on providing security, but it appears that communications throughput does not tend to be high when VPN communications are carried out.

SoftEther VPN is optimized to exhibit high performance for any line from low speed lines, ISDN and PHS to high speed lines such as 100Mbps and 1.0Gbps. For example, it can be exhibit throughput of several hundred Mbps for a computer with a Pentium 4 2.8GHz processor currently available for a low price even by using a VPN Server.

Problems like decline or marked delay in throughput due to re-transmission of TCP/IP protocol previously is used for tunnel communications for VPN which has been discussed in several theses, has been improved by technology to establish multiple parallel TCP/IP connections between VPN Server and VPN Client or with VPN Bridge. For details see 4.4 Making Connection to VPN Server.

1.1.8 Advanced Function and Expandability

Many older VPN products only realized VPN communications. For example, advanced function such logging all packets flowing inside VPN, conducting packet filtering inside VPN communications, or applying a highly flexible security policy are extremely rare.

With SoftEther VPN, software of VPN Server, VPN Client, etc., are equipped with extremely advanced functions. For example, the following functions can be easily set and used, and can be used for limiting VPN communications, network administration or other purposes.

- Flexible adjustment of communication parameters of SoftEther VPN protocol
- Logging VPN operation log or the contents of some packets
- Advanced security functions
- VPN communications monitoring
- Handling large environments by clustering
- Flexible user authentication
- Layer 3 switching function, virtual NAT and virtual DHCP server function
- Administration automation
- Others

Details concerning these functions are provided in other sections of this chapter and 2. SoftEther VPN Essential Architecture, 3. SoftEther VPN Server Manual and 4. SoftEther VPN Client Manual, etc.

With SoftEther VPN, the majority of these functions are provided in software rather than certain hardware. The internal program structure is meticulously formed into modules thus facilitating addition of new functions in the future, and this will be much more expandable than hardware-based VPN solutions.

1.1.9 Platform Independence and Interchangeability

SoftEther VPN currently supports various types of operating systems and CPU combinations so it can run on various platforms. With the exception of a few limitations, SoftEther VPN works the same without dependency on CPU type or platform such as Windows, Linux, FreeBSD, Solaris and Mac OS X.

The SoftEther VPN program code is written in highly interchangeable C and is programmed so as not to be dependent on a certain operating system. SoftEther VPN currently supports the operating environment indicated in Specifications, but will be supporting even more operating systems and CPU hardware in the future. Also facilitates integration of network appliances such as routers and firewalls.

SoftEther VPNs that operate in various environments can also be reliably connected with each other via the Internet. Thus if you construct a VPN that using SoftEther VPN, when

the number of systems or devices that supports SoftEther VPN increased, mutual connect ability will be technically maintained with the systems.