1.6 VPN Communication Details

This section contains a brief description of basic concept of various matters involving VPN communication using SoftEther VPN and a description of important things to know when constructing VPN by SoftEther VPN.

1.6.1 VPN Sessions

With SoftEther VPN, VPN communication starts when the VPN connection source computer connects to the VPN Server by VPN. This unit of VPN communication is referred to as a "VPN session".

In 1.4 VPN Processing Principle and Communication Method, it was explained that along with emulating a conventional Ethernet switching hub, SoftEther VPN can be a accept connection from a VPN connection source just as a physical connection point of a conventional switching hub.

Physical network adapters and switching hubs are connected to each other by network cable. But SoftEther VPN are being ready just in case, when a Virtual Network Adapter or Virtual Hub of another computer is connected to a Virtual Hub, the communication contentions are tunneled and flow through a physical network as TCP/IP-based SoftEther VPN protocol. Consequently each and every SoftEther VPN protocol connections are substantially, same as a network cable for physical Ethernet, and it can be expressed as a connection unit for Ethernet.

With SoftEther VPN, when VPN Client connects by VPN to VPN Server or when Virtual Hubs connect to each other by cascade connection, a transmission path for VPN communications are established. And when encapsulated Ethernet frames are transmitted, a VPN session will be established between VPN connection source and VPN Server in all cases. In addition to this, although it does not physically exist, virtual hosts or DHCP servers which is connected to a Virtual Hub by software is internally generating the VPN sessions.

For more information on VPN sessions, see the rest of this chapter and 3.4 Virtual Hub Functions, etc.

1-6-1.png

Various VPN session types from perspective of Virtual Hub.

As it will be subsequently explained, the following seven types of sessions exist for SoftEther VPN. Concerning each respective session, with the exception of some special treatment, the Virtual Hub will handle all by the same mechanism.

Type	Session name	Generator
Ordinary session	**Client mode session**	Conventional VPN connection from VPN Client
	Bridge/router mode session	Conventional VPN connection from VPN Client Cascade connection from VPN Server Cascade connection from VPN Bridge
	Monitoring mode session	Conventional VPN connection from VPN Client
Special session	**Local bridge session**	Local bridge function in VPN Server
	Cascade connection session	Cascade connection function in VPN Server
	SecureNAT session	SecureNAT function in VPN Server / VPN Bridge
	Virtual layer 3 switch session	Virtual layer 3 switch function in VPN Server

1.6.2 Accepting Connection by VPN Server

SoftEther VPN Server is the only software that can accept the VPN connection session from SoftEther VPN Client, SoftEther VPN Server and SoftEther VPN Bridge running on another computer.

SoftEther VPN Server stands by for the connection with multiple TCP/IP ports open as a port number for accepting VPN connection from the VPN connection source computer. The list of port numbers that are used can freely be established or modify by the VPN Server administrator .

The TCP/IP port numbers which to open the stand by for VPN connection from other computers are called "listener ports". The following three TCP/IP ports are allocated as listener ports by default.

- Port No. 5555 (This port number is used exclusively by SoftEther VPN; the number 5555 mean just for easy remembrance.)
- Port No. 443 (The number of This port number is the same that of "HTTPS protocol". It will be convenient for you to make relay equipment recognize TCP/IP connection as HTTPS protocol for VPN session.)
- Port No. 992 (This port number is the same port number as that of TELNETS protocol, which is now hardly used anymore. It will be convenient for you to make relay equipment recognize TCP/IP connection as TELNETS protocol for VPN session.)

By opening multiple TCP/IP ports, other computers that attempts to connect to that VPN server, SoftEther VPN Server will execut the connection to the easiest port number to connect to the according network environment, proxy servers and limitations such as firewalls. No matter which TCP/IP port you connect to, the functions and performance are the same after the VPN session has been established. SoftEther VPN Server will treat each TCP/IP listener port equally.

For more information on listener ports, see 3.3 VPN Server Administration.

1-6-2.png

TCP/IP listener ports of VPN Server.

1.6.3 Connecting to Virtual Hub

As it was described earlier in 1.4 VPN Processing Principle and Communication Method, SoftEther VPN Server can operate multiple Virtual Hubs within a single server process.

Computers that attempts to connect by VPN to VPN Server, it will chose the specific Virtual Hubs that is now available and operating in VPN Server.

When it is attempting to connect to a Virtual Hub, a user authentication, such as explained earlier in 1.5 Strong Security Features has to be carried out. A user information is managed separately for each Virtual Hub and it has to be set in advance by each SoftEther VPN Server and Virtual Hub administrator. As a result of carrying out user authentication, according to user information in the security account database that exists for each Virtual Hub, if the VPN Server recognizes the VPN connection as proper, the VPN Server accepts the VPN connection to the Virtual Hub, an new VPN session will be established and VPN communication will start.

During the time connecting to the Virtual Hub, there will be no VPN communication between the VPN connection source computer and VPN Server (sending/receiving of Ethernet frames); VPN data communication wil be carried out after user's authentication has been completed. Processing during connection to Virtual Hub before completion of user's authentication by SoftEther VPN protocol during negotiation VPN is actually completed, session is established, and state where VPN communication can be used is expressed as "established".

1-6-3.png

VPN protocol sequence and status transition at time of connection to Virtual Hub and session establishment.

1.6.4 TCP/IP Communication of Session Data

With SoftEther VPN protocol, packets that flows through the actual physical network for communication between SoftEther VPN Server and VPN connection source computer (VPN session) are encapsulated as TCP/IP packets and are generated by sender. The TCP/IP packets that is received by the reception side will be encapsulated and de-capsulated. All TCP/IP communication is encrypted by Secure Socket Layer (SSL) and an electronic signature can be added.

For communication between SoftEther VPN Server and VPN connection source computer, communication can be carried out by one TCP/IP connection per VPN session. When the user so desires, multiple TCP/IP connections can be established and the load distribution can be performed for communication data among these TCP/IP connections. Also the delay can be managed, transmission sequence automatically adjusted, network line used more efficiently, throughput and response enhanced. Data transmission direction (full duplex or half duplex) and life until cut off can also be set for each TCP/IP connection. For details see 2.1 VPN Communication Protocol and 4.4 Making Connection to VPN Server.

All data contents for data transmission of SoftEther VPN protocol is encrypted by SSL and it is compressed by a data compression algorithm. When it is used for low-speed lines such as modems or ISDN or PHS, data compression may theoretically function

effectively while transmitting in large quantities of data. Compression can be used simultaneously with encryption. For more information on data compression, see 2.1 VPN Communication Protocol and 4.4 Making Connection to VPN Server.

1-6-4.png

Virtual Ethernet frame transmission in VPN session.

1.6.5 Association with MAC Address

Virtual Hub manages multiple VPN sessions from VPN client connection sources, receives virtual Ethernet frames sent to Virtual Hub from those sessions, identifies destination MAC address and sends them out to other proper VPN sessions. This processing is the equivalent of layer 2 Ethernet frame switching (packet exchange) carried out in a physical switching hub.

Just like a physical switching hub, Virtual Hub automatically conducts MAC address learning and associates the learned MAC addresses with VPN sessions. When Ethernet frames that is needed to be processed arrive, the destination MAC address of the Ethernet frame can be read and switched to a suitable matching VPN session. This virtual Ethernet frame switching processing is the most important function of Virtual Hub and it is the most substantial part of VPN communications by SoftEther VPN.

MAC address tables which is managed by Virtual Hub are automatically updated and it's actual network status is applies as much as possible. The Virtual Hub administrator can display the MAC address table an can freely delete entries.

The mechanism and timing by which Virtual Hub learns new MAC addresses and update the MAC address table database is the same as that of a physical Ethernet switching hub.

1-6-5.png

VPN session and MAC address association by Virtual Hub.

1.6.6 Session from other VPN Server / VPN Client / VPN Bridge

SoftEther VPN Server accepts connection from software that is compatible with SoftEther VPN protocol that is running on other computers (there will be no problem even if running by localhost). There are three types of this software: SoftEther VPN Server, SoftEther VPN and SoftEther VPN Bridge (new software or dedicated hardware that supports SoftEther VPN may be developed and offered by SoftEther VPN Project or third party in the future).

1-6-6.png

Session from other VPN Server / VPN Client / VPN Bridge.

All VPN connections from these three types of softwares are conducted by SoftEther VPN protocol; the communication contents and nature are the same regardless of the type of software and purpose of communication.

Connection from SoftEther VPN Client

Connection from SoftEther VPN Client is generally connection from Virtual Network Adapter attempting to connect to Virtual Hub. In other words, when VPN Client is installed on client computers of end users using VPN communications and VPN Server is registered as the connection destination of VPN Client, the Virtual Network Adapter of the computer connects to Virtual Hub operating by VPN Server, and it can carry out the same communication as for example a network adapter connected to a physical switching hub by network cable.

As a special usage method, it is going to be possible to bridge connection by layer 2 between VPN Client computer Virtual Network Adapter and existing physical network adapter connected to the computer. As for, the bridge function of the operating system is going to be use for this. With SoftEther 1.0, bridging between Virtual Hub and physical network adapter has been often accomplished by this method. With SoftEther VPN, however, because bridging could be accomplished easier and faster by local bridge connection function of VPN Server or VPN Bridge, this method ceased to be used frequently.

Connection from SoftEther VPN Bridge

Whele SoftEther VPN Bridge operating at a base in remote location, it can be connected to SoftEther VPN Server by cascading the connection. By connecting the two Virtual Hubs on the VPN Server and VPN Bridge sides to existing physical LAN of both bases, you will be able to connect the two bases by VPN connection. This method is often used for base-to-base VPN connection.

For more information on SoftEther VPN Bridge, see 5. SoftEther VPN Bridge Manual.

Connection from SoftEther VPN Server

Because SoftEther VPN Bridge is software that limits just one part of SoftEther VPN Server, as it has been described ealier, the connection method from SoftEther VPN Bridge works the same for cascade connection from one SoftEther VPN Server to another and it can be used as such.

1.6.7 VPN Session Connection Modes

As it is explained in 1.6.6, VPN connection of VPN Client / VPN Server / VPN Bridge, etc., operating on another computer to VPN Server will established and managed as a VPN session for all Virtual Hubs.

VPN Server is basically treated as same for VPN sessions of any SoftEther VPN protocol, but that does not mean it is interested in the type of VPN software of the VPN session connection source or the type of network of the VPN session destination.

To facilitate administration of the VPN network of SoftEther VPN Server, you may want to differentiate and separate the connection type of the connection source computer of VPN session, into two types according to the objective of VPN session. Thus SoftEther VPN adopts the concept of connection mode for ordinary VPN session and defines two types of connection modes.

Connection modes include a client mode and a bridge/router mode.

1.6.8 Client Mode Session

VPN session in the client mode is primarily applied to VPN sessions that is connected from VPN Client to VPN Server. In this way of using conventional VPN Client, it will primarily usage as VPN client for remote access VPN by installing VPN Client on client computers in a remote location, that can creat Virtual Hub and connecting the Virtual Hub to VPN Server.

Therefore with VPN sessions that are established by connection from conventional VPN Client, only one Ethernet device with a MAC address should be connected to VPN on the VPN Client side. In other words, Virtual Network Adapter device driver that is used by VPN Client for connection, is simply connected to Virtual Hub, and the MAC address will allott to the Virtual Network Adapter in which is supposed to be the only network adapter existing on the client side for the concerned VPN session.

Users who actually use computers installed with VPN Client, however it can bridge connected to a separate physical network adapter on the client computer side by using function of the operating system and it can connect to another IP network by using the IP routing function of the operating system. If this operation is randomly performed by users who is having VPN Client, the user may unintentionally alter the network topology on the VPN administrator side, and they could destroy the uniformity and manageability of the VPN network as a whole.

Thus in a client mode session (i.e., VPN session connected from VPN Client layer 2 bridge or layer 3 routing on the client side of the VPN session), it is forbidden as a rule. This makes it impossible for users of VPN Client connected to SoftEther VPN Server to connect Virtual Network Adapter on the client computer side to another network. In other words alteration of the network topology or unintentional computer connection to VPN by administrator can be prevented.

By selecting the bridge/router mode as the connection mode for advanced communication setting of VPN Client connection settings, client mode session limitations are canceled so the bridge and routing on the VPN Client side become possible. For details see 4.4 Making Connection to VPN Server.

If deny security policy bridge and router operation a enabled for user setting values registered for each Virtual Hub of SoftEther VPN Server, users cannot connect to VPN Server in bridge/router mode (error occurs for VPN connection). For more information on security policy, see 3.5 Virtual Hub Security Features.

1-6-7.png

Client mode session and bridge/router mode session.

1.6.9 Bridge/Router Mode Session

If VPN session is connected by bridge/router mode session, the limitation whereby layer 2 bridge and layer 3 routing are denied on the VPN connection source side for client mode sessions and as a rule any kind of communication can be carried out.

The session connection mode is automatically selected when Virtual Hub of SoftEther VPN Server or SoftEther VPN Bridge are connected to a separate Virtual Hub by cascade connection.

Setting on the VPN Client side is required to connect to from SoftEther VPN Client to Virtual Hub in the bridge/router mode. For details see 4.4 Making Connection to VPN Server.

The administrator must establish security policy so the user can't connect to Virtual Hub created for use with general VPN connection in the bridge/router mode. For more information on security policy, see 3.5 Virtual Hub Security Features.

1.6.10 Monitoring Mode Session

The monitoring mode is a connection mode that can be selected when VPN Client connects to Virtual Hub of VPN Server.

VPN sessions connected in the monitoring mode can receive all Ethernet frames flowing through the connection source of Virtual Hub as they are. This mode can be used for intercepting Ethernet packets which flowing through Virtual Hub, capturing them using packet capture software, and inspecting all packets such as IDS and IDP. Sessions connected to Virtual Hub in the monitoring mode can receive all Ethernet frames flowing through Virtual Hub, but Ethernet fames cannot oppositely be transmitted to Virtual Hub.

Using this mode enables you to execute the equivalent of functions such as port monitoring and port mirroring which common layer 2 intelligent switching hubs are equipped with.

1-6-8.png

Monitoring mode session.

1.6.11 Local Bridge Session

A local bridge session is established when a local bridge connection has created it between Virtual Hub of SoftEther VPN Server and a physical network adapter. Unlike a conventional VPN session established by VPN connection from VPN Client / VPN Server / VPN Bridge by SoftEther VPN protocol via a network, the actual communication source for local bridge sessions is a module separate of the computer on which operating VPN Server, also it is therefore classified as a special session.

For more information on these functions, see 3.6 Local Bridges.

1.6.12 Cascade Connection Session

A cascade connection is a special session generated within a Virtual Hub of cascade connection source VPN Server or VPN Bridge if Virtual Hub of SoftEther VPN Server or SoftEther VPN Bridge operating on a separate computer which is connected to Virtual Hub of SoftEther VPN Server by cascade connection.

In other words, in the case of using cascade connection, a bridge/router mode session, which is the normal session, will generated by the Virtual Hub of the side being connected to, and a cascade connection session, which is a special session, will creat by the Virtual Hub which initiated the cascade connection.

For more information on cascade connection sessions, see 3.4 Virtual Hub Functions.

1.6.13 SecureNAT Session

A SecureNAT session is a special session that has automatically created internally when the SecureNAT function, which is one of the Virtual Hub functions of SoftEther VPN Server or SoftEther VPN Bridge, is enabled. For more information on SecureNAT function, see 3.7 Virtual NAT & Virtual DHCP Servers.

1.6.14 Virtual Layer 3 Switch Session

A virtual layer 3 switch session is a special session that has automatically created internally for connection between virtual layer 3 switch and Virtual Hub when virtual layer 3 switch function, which is a function of SoftEther VPN Server, is used. For more information on virtual layer 3 switch function, see 3.8 Virtual Layer 3 Switches.

See Also

- 1.4 VPN Processing Principle and Communication Method
- 1.5 Strong Security Features
- 2.1 VPN Communication Protocol
- 3.3 VPN Server Administration
- 3.4 Virtual Hub Functions
- 3.5 Virtual Hub Security Features
- 3.6 Local Bridges
- 3.7 Virtual NAT & Virtual DHCP Servers
- 3.8 Virtual Layer 3 Switches
- 4.4 Making Connection to VPN Server
- 5. SoftEther VPN Bridge Manual