2.1 VPN Communication Protocol

The protocol used by SoftEther VPN for VPN communications are version 3 of the global security standard Secure Socket Layer (SSL). SoftEther VPN includes several technical innovations to increase speed and enhance security of VPN communications.

This section provides a detailed description of SoftEther VPN protocol. For more information on SoftEther VPN protocol, see 1.6 VPN Communication Details.

2.1.1 Communication Speed

SoftEther VPN is a VPN system that consists of exchanging virtual Ethernet frames and communicate by VPN among VPN Client / VPN Server / VPN Bridge. Based on TCP/IP protocol, SoftEther VPN protocol plays the role of encapsulating, encrypting and transmitting virtual Ethernet frames on a physical IP network.

Normally there is a problem that the drawback of communication that do not have much high efficiency in protocol based on conventional TCP/IP. This is because of the protocol itself conducts retransmission control and flow control, in some cases TCP/IP can only be used for some actual available network bands.

However, as for SoftEther VPN protocol, by dexterously controlling and optimizing TCP/IP connection establish carrying out to VPN communication while developing, communication will be optimized and be more efficient then ever. In the case where SoftEther VPN is used for a network with sufficient bandwidth, SoftEther VPN Project has succeeded in realizing higher speed and lower delay for so the user of VPN communication that you would never sense a bit of difference in whether communication is carried out via VPN or directly flowing on a physical network.

2.1.2 Flexibility

SoftEther VPN protocol is based on TCP/IP and all data flows according to TCP/IP connection. When constructing VPN by SoftEther VPN, it can be constructed via network devices and servers that support TCP/IP.

VPN can now be easily constructed through proxy servers, NAT or firewalls that used to be difficult for VPN protocol, representative examples of which as older PPTP or L2TP/ IPSec.

For method of actually conducting stable VPN communications through a proxy server or other firewall, see 4.4 Making Connection to VPN Server.

2.1.3 Communication Efficiency and Stability

Communication efficiency (throughput and response) and stability can be enhanced for the following networks when the user properly sets advanced communications parameters of SoftEther VPN protocol.

- Networks with large delay time despite wide bandwidth.
- Networks whereby there are proxy servers, NAT or firewalls in the VPN communications route that produce the delay.
- Networks whereby there is band control equipment (QoS equipment) on the VPN communications route which intentionally band control maximum communication speed for each separate TCP/IP connection.
- Networks whereby there are proxy servers, NAT or firewalls in the VPN communications route, special processing for TCP/IP protocol through network gateway devices and servers that are executed, an expiration date is set for each TCP/IP connection and the connection is disconnected when the expiration date is exceeded, count and transmission interval for packets of HTTPS protocol, etc., will be strictly recorded, and if there is a violation of the default standards of HTTP protocol, the TCP/IP connection will be disconnected and special processing be executed.

VPN communication source computers will simultaneously establish multiple TCP/IP connections for a single VPN session with SoftEther VPN Server, and by distributing load for communications data by using the respective connections in parallel, VPN communication data can be sent and received at high speed with low delay by SoftEther VPN protocol.

Communication of VPN session by multiple TCP/IP connections.

Computers that connects to VPN communications can initiate VPN connection by specifying the following parameters.

Reconnection Setting when VPN Connection Fails or Becomes Disconnected during Communications

If the VPN connection to SoftEther VPN Server was temporarily cut off due to network problems or the connection destination VPN Server stops (temporarily), the system will attempts to reconnect to the VPN Server until it will succeed. You can specify the maximum number of reconnection that attempts to and the interval at which reconnection is attempted (cannot be set less than 5 seconds).

As for the default setting, it is 15 seconds for reconnection attempt by interval and number of reconnection attempting is unlimited. The connection will be maintained constantly as long as the network is functioning and connection destination VPN Server is runnig.

As for the cascade connection, while attemptions are made to connect the SoftEther VPN Server and connection is completed, the function to maintain connection keeps the reconnection interval will be fixed to 10 seconds and the number of reconnection will attempt to be fixed to unlimited. The user does not have a permission for this change nor settings.

VPN session type, reconnection interval, number of reconnection attempts that can be set and the default settings are as follows:

Session type	Reconnection interval	Number of reconnection attempts
Ordinary VPN sessions initiated by VPN Client	Min. 5 seconds (default is 15 seconds)	0 - unlimited (default is unlimited)
Cascade connection VPN sessions initiated by VPN Server / VPN Bridge	10 seconds (fixed)	Unlimited (fixed)

Number of TCP/IP Connections Used for VPN Communication

Multiple TCP/IP connections can be established during VPN session with SoftEther VPN Server, therefore throughput can be enhanced and delay shortened using respective parallel TCP/IP connections for data transmission. Also if some of the established TCP/IP connections are disconnected or communication cannot be carried out for a certain amount of time, the number of insufficient TCP/IP connections can be compensated for by creating the new TCP/IP connections up to the specified amount, adding VPN sessions, and it will try to maintain as much as communication with the specified number of TCP/IP connections.

2-1-2.png

Automatic reconnection processing if disconnected while using multiple TCP/IP connections.

The user can set the TCP/IP connections number at the range of 1 to 32.

- Creating new connection settings by SoftEther VPN Client, TCP/IP connections number is 1 in default setting.
- Creating new connection settings by SoftEther VPN Server / SoftEther VPN Bridge, TCP/IP connections number is 8 in default setting.

If the number of TCP/IP connections is simply increased, rather than enhancing throughput of VPN communications, or the bandwidth of the communication route with the VPN Server on the IP network is large, it appears that increasing the number of connections often enhances throughput or stabilizes communication. Oppositely, in the case of low speed lines like ISDN or PHS where bandwidth is just server tens or hundreds of kbps, because of the band is consumed by Keep-Alive messages and control data of various TCP/IP connections, fewer connections often improved stability and enhances the communications speed.

The number of optimal TCP/IP connections furthermore varies according to the amount of data and type of communications protocol which is used within the VPN session. After actually constructing VPN, we will recommend you to select the proper setting while using the communication throughput measurement tool. For details on the communication throughput measurement tool, see 4.8 Measuring Effective Throughput.

Establishment Interval for TCP/IP Connections

If you are about to conducting VPN communications by establishing 2 or more TCP/IP connections, you can specify how many seconds must pass after the immediately preceding TCP/IP connection has been established before another can be established beginning with the second one. The default setting is 1 second. This can be set to longer then 1 second.

Normaly you do not have to change this number (1 sec). However when you are trying to connect large number of TCP/IP (such as 32 connection) continuously, this may occur some physical or IP network problem as it is default setting number (1 sec). The firewall or IDS may confuse this connection as a “Dos attack” or “physical attack”. So if you are about to connect large number of TCP/IP continuously, try use this manual setting to loger second then 1.

2-1-3.png

Establishment interval for TCP/IP connections.

Life of TCP/IP Connections

If you want to communicate VPN by establishing more then 2 TCP/IP connection, when TCP/IP connections are completed, between computer and VPN server TCP/IP

connection can be disconnected after the particular set seconds while can newly establish the shortage of TCP/IP connection. By default setting this function is disuse.

This function is used to stabilize VPN communications by SoftEther VPN protocol in an unstable network such as where network gateway devices on the IP network route such as firewalls, IDS or proxy servers, or if the server setting per TCP/IP connection is set to a long time, the connections may be disconnected or mistaken as a DoS attack, etc.

Using in Half Duplex Mode

The half duplex mode is a function whereby, if VPN communications are conducted by establishing 2 or more TCP/IP connections, concerning various TCP/IP connections between VPN connection source and SoftEther VPN Server, approximately half of the TCP/IP connections are dedicated to the transmission direction and the other half are dedicated to receiving. If this function is enabled, transmission direction of data flowing through respective TCP/IP connections established as part of SoftEther VPN protocol is limited to either from VPN server to client (download) or from client to VPN server (upload). If all TCP/IP connections are lumped together, simultaneous communication in both directions is possible (full duplex), but each respective TCP/IP connection can only handle data transmission in one direction, so it is referred to as the half duplex mode.

This function is used to stabilize VPN communications by SoftEther VPN protocol in an unstable network where the proper communication by SoftEther VPN protocol is mistaken as an attack or malicious backdoor communication and a warning is issued or disconnected forcibly, by the network security devices such as, firewalls, IDS or proxy servers on the physical IP network that inspect TCP/IP packets for bidirectional SSL data flow.

By using the half duplex mode, some software processing is involved for control processing, and because CPU time is consumed, communication speed efficiency deteriorates but drop in throughput and the effect on the user is extremely small, so there is no problem under ordinary circumstances.

2-1-4.png

VPN session communications in half duplex mode.

Disabling Encryption Option

By default with SoftEther VPN protocol, all communications contents are encrypted by SSL and an electronic signature is added, but in the following cases encryption and electronic signature can be waived.

- If physical IP networks that conduct VPN communications are limited to physically secure LAN and it is physically difficult for a malicious third party to eavesdrop on and/or tamper with packets on the line.
- If communications are conducted by dedicated frame relay offered by communications provider or on a network with high reliability whereby eavesdropping by other users is difficult such as wide area Ethernet and the service provided by the communications provider is sufficiently reliable.
- If SoftEther VPN protocol is combined with other software (SSH port transmission tool, etc.) and encryption has been carried out the lower layer.
- If the same computer is operating between VPN connection source software and SoftEther VPN Server (case where connected to localhost). The connection configuration such as this results when cascade connection, etc., is conducted among Virtual Hubs of the same VPN Server.

By not executing encryption and electronic signature, a header for encapsulating is simply added to virtual Ethernet frames for data flowing on a physical IP network, and encryption and electronic signature protection is not implemented by SoftEther VPN protocol. Thus more CPU time for calculating encryption and electronic signature can be used for encapsulating virtual Ethernet frames and communication to enhance communication throughput.

Even if encryption is disabled, important processing such as user authentication is encrypted by SSL.

Using Data Compression

SoftEther VPN protocol can compress sent and received all Ethernet frames internally and transmit them. The deflate algorithm developed by Jean-loup Gailly and Mark Adler is used as the data compression algorithm. The compression parameter is set so processing is executed at the fastest speed.

By using data compression for VPN communications, a maximum of 80% of communications volume can be reduced (depends on protocol used). If compression is conducted, CPU load of both client and server becomes higher, and depending on the performance of the various types of hardware, if the line speed exceeds about 10 Mbps, in many cases not compressing data improves communication speed.

2.1.4 Encrypted Communication Security

With SoftEther VPN protocol, encryption and electronic signature are realized using SSL. The following are implemented as the encryption and electronic signature algorithm used.

- **RC4-MD5**
- **RC4-SHA**
- **AES128-SHA**
- **AES256-SHA**
- **DES-CBC-SHA**
- **DES-CBC3-SHA**

The algorithm used for encryption is specified by the SoftEther VPN Server administrator (cannot be specified by connection source computer users). You can select any of the encryption algorithms given above, but RC4-MD5 is selected by default.

RC4-MD5 is the fastest algorithm that offers a certain degree of security. There is no need for you to select another algorithm without a special reason. In a service environment where only a certain algorithm such as AES can be used due to regulations or an administrator that is stricted about encryption, you can use a more secure encryption algorithm such as AES.

2.1.5 Support for VoIP / QoS

SoftEther VPN protocol supports QoS for VPN communication and gives band priority to high priority packets such as VoIP packets for transmission processing. For details see 1.9 VoIP / QoS Support Function

See Also

- 1.6 VPN Communication Details
- 1.9 VoIP / QoS Support Function
- 4.4 Making Connection to VPN Server
- 4.8 Measuring Effective Throughput