4. Fast Throughput and High Ability

4.1. Highly Optimized VPN Processing Modules

SoftEther VPN has highly optimized VPN processing modules on its core with written by C language strictly. The architecture of it is modern-designed in order to exercise the best performance with nowadays Internet broadband connections.

Comparisons

Legacy VPN protocols, such as L2TP or PPTP was inherited from the bad behavior of the antique protocol, PPP (Point to Point Protocol). PPP was designed for purpose to transmit packets via narrowband telephone lines. It is not good for contemporary high-speed Internet lines.

According to the study which was conducted at University of Tsukuba in 2006, the throughput of SoftEther VPN is 4 times faster than Microsoft's PPTP VPN. And also it is 13 times faster than OpenVPN. Almost all of other VPN protocols and implementations are not well-written for demonstrate high-speed throughput.

Why SoftEther VPN Exercise so Faster?

SoftEther VPN was developed for the aim to realize high performance. Other VPNs was developed for only the purpose of ensuring the security. SoftEther VPN had both purpose of security and performance. So the architectures of VPN processing are totally different.

Reducing the Frequency of Memory Copies

Copying the contents of memory always decreases the speed of programs. SoftEther VPN was developed with cautions to reduce the count of memory copies per each cycle of processing a VPN packet.

Resolving the MTU Problems

Computers use 1,514 bytes as MTU (Maximum Transmission Unit) by default, because it is a standard of Ethernet packet size without FCS. And it is virtually no way to determine the optimized size of MTU even it a packet is transmitted via VPN.

Legacy VPN protocols, such as IPsec, PPTP and L2TP, are not good for this Ethernet MTU value. There is a serious problem, called "MTU Problem" with legacy VPNs which is came from the limitation that legacy VPNs must transmit packets into tunnels which consist data grams in physical line.

If a computer transmits a full size of packets (1,514 bytes) via the Ethernet segment, it will realize the best throughput. But if there is a legacy VPN between two computers, the performance will be almost half. Each packet will be divided into two packets due to MTU problem. Increasing the total number of packets will decrease the total throughput.

Ideally, this problem has to be solved by both Path MTU Discovery Protocol and appropriate settings on the edge nodes. But Path MTU Discovery is useless in the actual network. And set up appropriate MTU settings on all computers on the network is impossible.

Unlike legacies, SoftEther VPN adopts streaming tunneling mechanism. SoftEther VPN will optimize the burst-sending packets with filled all of 1,514 bytes to transmit via VPN tunnel. Packets will be joined as a queued sort of packets and regarded as a single entire block. And SoftEther VPN will capsule the entire block by HTTPS and SSL, and finally it will be sent to the physical network. Then few increasing of number of packets will be occurred in the process of tunneling. This artifice method keeps a good performance.

4.2. Parallel Transmission Mechanism of Multiple Tunnels

To realize a good transparency for firewalls, proxies and NATs, SoftEther VPN adopts HTTPS protocol for physical transmitting. But HTTPS is on TCP, and TCP is not good if there are terrible packet-losses and packet-delays.

Then SoftEther VPN adopts additional extensions to HTTPS protocol. It is called "Parallel Transmission Mechanism" . User can set up the number of concurrent parallel transmission channels 1 to 32. In the environment such as slow and delaying network, this performance tuning will return good results for throughputs.

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 health VPN connection. This fast-switching optimization to determine the processing TCP connection enables high throughput.

4.2.jpg

A logical VPN session consists of multiple TCP connections to improve throughput over high-latency network.

ss4.2.jpg

You can specify the number of concurrent TCP connection to construct a logical VPN session.

4.3. Away from the Firewall's Eye, Camouflage as an Usual HTTPS Session

Some smartest firewalls in contemporary market can detect the abnormal behavior of TCP connections which passes through the firewall. If there in such firewall in the exit to the Internet on the network, a VPN Session of SoftEther VPN might be detected as abnormal TCP connection and also might be terminated by the firewall. It will be a risk to keep a reliable and stable VPN Sessions.

Because SoftEther VPN exploits HTTPS protocol as a tunnel for transmitting inner packets of VPN, a HTTPS/TCP connection will be bi-directional. In the standard behavior of HTTPS, there are the maximum numbers of the switching of the direction in the same TCP session from the establishment of the session to the termination of it, standard values is 15 as defined in RFC of HTTP 1.1 protocol. If SoftEther VPN uses a single HTTPS/TCP connection for purpose of tunneling, the number of switching the direction must exceed 15. That is impossible of normal HTTPS usage. Then a smart firewall, which has state-full-packet-inspection-function, will disconnect that HTTPS session.

To reduce this risk to be detected as abnormal connection, SoftEther VPN has two ways. First, SoftEther VPN divides all TCP connections, which is consisted for a logical VPN Session, into two groups. First group is for uplink only and another group is for downlink only. This cheap trick must help hiding the abnormal behavior. Secondly, SoftEther VPN sets the life-time for each of all TCP connections. The firewall might detect a too-long-alive TCP connection as abnormal and terminate it. Before that, SoftEther VPN will end a TCP connection's life voluntary and establish new one.

These two mechanisms can help preventing the VPN Session to be detected as abnormal by state-full-packet-inspection firewalls.

4.3.jpg

A logical VPN session consists of many TCP connections.
Each TCP connection has very short-term lifetime.
The firewall in the path of traffic cannot identify them as a VPN session.

4.4. Virtual NAT and Virtual DHCP Server

It is best way to place a DHCP Server on the Ethernet segment to assign IP addresses to VPN Client from the pool automatically. But if you don't want to pay any cost to set up and place a DHCP Server on the Ethernet segment, alternatively you can set up the Virtual DHCP Functions on the Virtual Hub. Virtual DHCP Server serves as a real DHCP server. The function is limited, but you can enjoy standard DHCP functions from it.

Virtual NAT Function is also implemented on the Virtual Hub. This function is helpful when you cannot use Local Bridge functions, but you still want to access to the physical LAN from the Virtual Hub, such as remote accessing VPN. Virtual NAT works on the user-mode of the computer and not depended on any kernel-mode drivers. So if SoftEther VPN Server's installation as system privilege is restricted, you can still enjoy accessing to the physical LAN with Virtual NAT function.

Please note that Virtual NAT function is implemented for limited purpose, such as temporary use or emergency case. It is not recommended to use it as daily business purpose.

A combination of both Virtual NAT and Virtual DHCP Server is called "SecureNAT" in the Virtual Hub.

ss4.4_2.jpg

Virtual NAT and Virtual DHCP Function Setting Screen

ss4.4_1.jpg

You can specify properties of virtual IP interface for Virtual NAT & DHCP Server Function.

4.5. QoS Support

QoS (Quality of Service) is supported in order to mark VoIP packets as highest-priority packet. You can enable QoS to make the voice-quality flowed via the VPN more clearly in the situation when other heavy-volumes of downloading of data are transmitted on the same VPN.

4.6. Packet Delays, Jitters and Losses Simulator

SoftEther VPN's Virtual Hubs can generate packet delays, jitters and packet-losses for a purpose of simulating the physical bad-condition networks. This function is useable if a network designer wants to examine what will be happened if something delays, jitters or packet-losses will be occurred, in the laboratory.

ss4.6.jpg

Delay and Packet Loss Generator.

4.7. Clustering

SoftEther VPN Server can construct the cluster farm. This means that two or more computers with SoftEther VPN Server installed can become a group for serving as if there is only a single VPN Server.

Load Balancing

If you create a cluster between several VPN Servers, then all VPN Sessions from VPN Clients will be balanced to members of the VPN cluster. Without load balancing, you can only host a few thousands of VPN Sessions on a VPN Server. But load balancing will make it possible to host several ten thousands of VPN Sessions, if the capacity of hardware allows it.

Fault Tolerances

In a VPN cluster, if a member server of cluster will functionally down due to trouble of hardware, all VPN Sessions which were connected on that member server will be redirected to other healthy member servers. There is nothing to be done by both users and administrators.

ss4.7_1.jpg

A VPN Cluster consists of many number of Cluster Member VPN Server.

ss4.7_2.jpg

Building a Cluster is easy. It can be done in just GUI settings.

4.8. Full IPv6 Supports

SoftEther VPN supports IPv6. It means that not only every security and management functions such as packet filtering can process IPv6 packets adequately, but also physical VPN tunnel of the VPN Session can be established on the IPv6 Internet.
For example, while the ISP supports only IPv6 for wide-area communications, but you can establish SoftEther VPN Session via IPv6 backbone-network and you can flow any kinds of Ethernet packet on that VPN Session, including IPv4.
It is easy to establish IPv4 on IPv4, IPv4 on IPv6, IPv6 on IPv4 and IPv6 on IPv6.

ss4.8_1.jpg

Virtual Hub fully understands IPv4 and IPv6.

ss4.8_2.jpg

You can define IPv6 Packet Filter Rules on Virtual Hub, as same as IPv4.

4.9. Throughput Test Tools for both Physical and VPN

To prove the actual throughput both via VPN and raw on physical network, it is good to use the throughput testing tool which is attached to SoftEther VPN as a free gift. Without any products of measurement of traffic throughputs, you can test a speed by this free and sufficient tool.

ss4.9_1.jpg

Network Traffic Speed Test Tool. Convenient for measuring both Physical and Virtual network capabilities.

ss4.9_2.jpg

An Example of Results of Traffic Speed Test Tool.