3. Security and Reliability

3.1. Excellent Security and Reliability, Superior to Hardware

You might have a question that whether SoftEther VPN is really secure as same as hardware VPN products or not.
Someone might think that software VPNs is inferior to hardware VPNs. Of course, SoftEther VPN is implemented as a software code, not hardware as either specific integrated circuit. But it is absolutely correct that SoftEther VPN has an adequate security fulfillment as same as hardware's one, and moreover it might be superior to hardware VPN.

What is Hardware VPN Products?

Please see the fact that almost all hardware VPNs on the today's market is not a pure hardware. They are nearly software program, actually. Do you have any experience to open the top cover of any Cisco Router? You can see that inside devices on the Cisco Router is almost same as today's computer. The major differences are only the architecture of CPU. To reduce the manufacturing cost, Cisco and other VPN vendors adopts cheaper CPU than computers, such as MIPS, ARM and PowerPC. Anything more important differences are there between a desktop computer and a hardware VPN router. And you can analyze the inside mechanism of Cisco Router by some information leaked from the Internet or books. Cisco VPN Router and other manufacturer's router are running the software operating system on their device. On the operating system, the routing and VPN session-managing software is also working to process VPN communication. Virtually almost all important processes are implemented as software, not as hardware, on the existing hardware VPN products in the today market. You can prove this thing about asking some friend in such a hardware company.

No Differences of Encrypting Strength between Hardware ASIC and Software Programs

It must be mentioned that some expensive VPN Router hardware products, such as Cisco VPN Concentrator, has ASIC (application-specific integrated circuit) for encryption and decryption of packets. Someone has misunderstanding that encryption processing by ASIC is more secure than processing by software programs. But it is absolutely wrong. The consequence of encryption and decryption are exactly identical between ASIC and software. And there is no weak-point in software processing of encryption at all, because all cipher algorithms are truly same no matter whether on ASIC or software. For example, Cisco's ASIC encryption processing unit implements AES-256, which is a standard cipher specification published by U.S. government. AES-256 is implemented as software code too, and the strengths of both are accurately same. Please do not confuse that ASIC is more secure than software processing module in an aspect of cryptology science.

SoftEther VPN is Certainly Safer than Legacy Hardware VPN Products

It is no exaggeration to say that security strength of SoftEther VPN is superior to legacy hardware VPNs. As you know, Cisco Systems and other legacy VPN vendors hide their code of both software and ASIC, so anyone can exanimate whether the inside steps of codes are really safe or not, and whether they implemented the secret backdoor in the product in order to allow anyone who knows a secret (for example, the government of theirs, or themselves) to enter a customer's private network without customer's permit or not. Anyone can prove the existence of such of security risks. Due to the fact that all internal software codes are written in the hardware ICs, we cannot do any reverse-engineering against it. These facts can say that legacy hardware VPNs has no certainly security to customers.

And in legacy VPN hardware products, the developer of operating system layer and the developer of VPN layer are the same vendor. This character will be vital security problem. In any codes, there must be some unknown vulnerabilities. Operating system layer is very large and complicated than VPN layer in the system. Then more vulnerability will be discovered in the operating system layer rather than VPN layer in future. Their closed and dedicated operating system is on their hand at all. So unless they decide to fix it and distribute a patch to all existing users, everyone will be affected but there is nothing to do users can. This case is very dangerous.

Two Reasons Why SoftEther VPN is so Secure than Hardware Vendor's VPNs

In comparison with hardware VPN products, SoftEther VPN can be said more secure, better than hardware products. There are two reasons. First, important parts of SoftEther VPN are now released as open-source software since 2010. Then the developer of SoftEther VPN cannot implement any backdoors on the software. It is impossible, because if the developer did it, anyone who analyzed the open-sourced code notice the implemented backdoor. So in the possibilities of existence of backdoor or some malicious code, SoftEther VPN is safer than other closed vendor's hardware VPN products.

Secondly, SoftEther VPN can run on many operating systems, such as Windows, Linux, FreeBSD, Solaris and Mac OS X. Today, these operating systems are very popular, so if a vulnerable weak-point is found on an OS, then someone will analyze it and post a patch code to publish. In the standard case, the major developer will publish and distribute the fix patch to everyone as free as fast as possible. You know about Windows Update system and Linux Distribution Update Program. SoftEther VPN's strong-point is that is completely separated to the operating system layer. Then all found security problems in the operating system can be solved in the operating system layer. Users have no risks that a developer is reluctant to fix the security issues on the operating system if a user uses SoftEther VPN. Using other legacy hardware VPN products has a risk of such a thing.

About Opening a TCP/IP Port on the Operating System for SoftEther VPN

In order to run SoftEther VPN Server on the server computer, you have to accept on particular TCP/IP port for incoming VPN connections. Generally, the port number is TCP 443 (HTTPS port).

Today's operating system has good software firewall features. It prevents any packets to any TCP/IP ports. Firewall functions are always turned on by default. So there are no possibilities to be passive from any attacks from the Internet's attackers and viruses. You have to open only the minimal TCP/IP ports in order to accept VPN sessions on the VPN Server. This is very secure, and no reason to say that using Windows or Linux for VPN purpose is dangerous.

3.2. Based on Internet Standard Protocols

SoftEther VPN adopts Internet Standard Protocols in all aspect of this software's communication functions via the Internet.

Upper Layer of VPN Tunneling Protocol

SoftEther VPN Protocol for tunneling is according to HTTPS (HTTP over SSL) Protocol. HTTP is today's most frequently used protocol for web browsing. HTTPS is an extension to ensure a security on HTTP. You might use SSL everyday on the Internet. There are no safer protocols than HTTPS in the world.

Intermediate Layer of VPN Tunneling Protocol

Both SSL 3.0 and TLS 1.0 are supported. User can choose which protocol to use. SSL is Secure Socket Layer protocol. TLS is Transport Layer Security protocol. Both of them are widely used in the Internet, and the safety and reliability are proved for more decades by standing despite everyone's mercilessly analysis who is engaging the cryptography science and industry.

Lower Layer of VPN Tunneling Protocol

Lower Layer of VPN Tunneling Protocol is according to TCP/IP, (Transmission Control Protocol on Internet Protocol), which is one of the Internet standard protocol. SoftEther VPN can use both IPv4 and IPv6 with TCP.

3.3. Supporting Many Cipher Standards

SoftEther VPN uses cipher algorithms for protect the VPN tunnel from attackers and information thieves on the Internet. A user can choose which cipher algorithms to be used. RC4 is faster but strength is not so good. AES256 is slower but virtually perfect strength.

Encryption and Deception Algorithms

The following cipher algorithms can be specified in SoftEther VPN. All of them are international standards.

- *RC4 (128 bits)*
- *AES128 (128 bits)*
- *AES256 (256 bits)*
- *DES (56 bits)*
- *Triple-DES (168 bits)*

RC4 is a stream algorithm and others are block algorithms.

Hashing Algorithms for HMAC

SoftEther VPN also uses hashing algorithms for HMAC (Hash-based Message Authentication Code) as follows. All of them are international standards.

- *SHA-1 (160 bits)*
- *MD5 (128 bits)*

3.3.jpg

ss3.3.jpg

Encryption algorithms setting screen.

3.4. Built on OpenSSL

The core engine of encryption, decryption and authentication in SoftEther VPN is based on OpenSSL. OpenSSL is most famous and authoritative open-source software library, widely used for every purpose which needs a security. No one can say that OpenSSL is not safer than something else.

This is advantage of SoftEther VPN. OpenSSL is well tried security implementation on the public and SoftEther VPN takes a benefit from it. Other legacy VPN's vendors develops their own crypto software code and using it on their products, because they don't want to use open-sources. It can be said that closed crypto codes are considerably weaker than opened one, according to common knowledge of cryptographic science.

Needless to say, SoftEther VPN uses OpenSSL with no modification to ensure the completeness of security.

3.5. Prevent Man in the Middle Attacks

"Person in the Middle Attacks" (as know as Man in the Middle Attacks) is widely known way to attack the encrypted session via the Internet. Middle Attacks can be prevented to validate the server's certificate by client. SoftEther VPN has a function to check it. All

VPN Server has its own RSA secret key and counterpart RSA public key within the X.509 certificate object. Every time VPN Client is being connected to the VPN Server, every time VPN Client can check the validity of the VPN Server's ID. And if anything is wrong, the VPN Session will be terminated immediately. No space for middle attackers.

ss3.5.jpg

SSL Server Verification detects and prevents Man in the Middle Attack.

ss3.5_2.jpg

Security Alert pop-ups when the destination VPN Server presents an untrusted SSL certificate.

3.6. User Authentication Methods

For ensuring the security, only encryption is not enough. User authentication is also mandatory to prevent invasions from unknowns. SoftEther VPN has several options for user authentication. It is suitable for from very small usage to large case for such as an enterprise that has several thousand employees.

3.7.jpg

SoftEther VPN supports external server user authentication methods.

Plain Password Authentication

The simplest method is the plain password authentication. In this method, a Virtual Hub on the VPN Server has a user database within it. The user database has multiple users and user's passwords. Password is hashed by SHA algorithms for security. An administrator can create a lot of users on the database. Each user has different passwords. No one who doesn't know the correct combination of user ID and password can connect to the Virtual Hub.

Authentication with Radius and Active Directory

The plain password authentication is simple and suitable for some purpose. But if a company has very huge numbers of employees and wants all of them to connect the VPN Server, it is inconvenient to define each user on the Virtual Hub. Such a company already has an external user authentication database. A company uses UNIX has Radius user-authentication server. A company uses Windows has Active Directory or NT Domain

Controller server. SoftEther VPN Server can be configured in order to relay the authentication process to such an external user-authentication database. If an administrator adopts this method, then he doesn't need to create each user for each employee on the Virtual Hub. It must reduce bothering tasks. There is another benefit. If a user changed the password of him or her, then the required password for connecting VPN Server will be changed. This means that a company can enforce employees to a particular password security preventing any attacks with password speculation from outside attackers.

From the reason that SoftEther VPN is according to the standard protocol of Radius, any modern user-authentication mechanism, such as one-time password tokens, can be used if that mechanism's authentication server is implemented to be compatible with Radius protocol.

ss3.6_1.jpg

RADIUS and Active Directory are supported for external user-authentication.

RSA Certificate Authentication as PKI up to 4096bits

Password authentication mechanisms don't provide adequate security for particular demands. Because user might forget passwords, so some users memorize the password on the post-it or notepad on theirs. Then the risk of password leakage will be increased.

Another alternative solution is to use PKI (Public Key Infrastructures). PKI uses RSA (Rivest, Shamir and Adleman) certificate files and its private key files. This way is also international standard.

If a user is specified to use PKI, a user doesn't need any passwords typing. Instead, a user must posses a private key. A private key can be held on both hard disks and security tokens.

ss3.6_2.jpg

RSA Certificate Authentication is easy to use.

Supporting Smart Cards and USB Tokens for PKI

It is safest way to use PKI with smart cards or USB tokens. Smart cards and USB tokens prevent the private key leakage from user, because such devices always require PIN number to access the internal private key. Moreover, at any time, anyone cannot read out the private key from such a device. Devices can only make a signature to given challenge random numbers. This mechanism is perfectly secure and no one can break this security. If you adopt this methods, highest security strengths is promised. Please note that not all smart cards and tokens are supported on SoftEther VPN. Supported device lists can be found on the web.

0509161.jpg

Any Smart Cards or USB Tokens which are compatible to PKCS#11 are supported.

Grouping Users

All user objects which are defined on the Virtual Hub by the administrator can be grouped. Groups can be created and a group can hold multiple users. It is very convenient to define the security policy or packet filtering policy to a group of several users.

3.7. Packet Filter

You can set up the packet filter rules on the Virtual Hub of the VPN Server. The number of rules can be placed up to 4096 entries. Packet filter function is also called "Access Lists" .

Any filtering ruling entry has the definition of behavior field to determine whether discarding or passing of the packet which is matched by the rule. And in the rest of the entry, you can specify the matching pattern for both IPv4 and IPv6 packets. A matching pattern can be not only IP addresses and masks, but also TCP and UDP port number ranges and TCP flags. And you can also specify the user name or group name of either source or destination of a packet.

You can redirect any HTTP connection request packets which are transmitted over the Virtual Hub, which are matched on a rule of the access lists. For example, an employee tries to access to the prohibited web site which is blacklisted on the access-lists. The Virtual Hub packet filter will automatically respond a "counterfeit" HTTP response packet to the client web browser. The client browser will treat the response packet as a redirection request from the destination server. Then the client user will see the URL which is specified by the administrator. (for example, the warning page with the picture of horrible angry face.)

ss3.7_1.jpg

Access Lists are easy-configurated on GUI Managerment Tool of VPN Server.

ss3.7_2.jpg

You can specify deep-level IP, TCP, UDP or other packets-header value to define a matching condition.

3.8. Security Policy

Many demands for restricting user's action can be fulfilled by packet filtering function. But some particular cases, you need more complicated rules to drop the harmful packets from users or other sites which have been connected via VPN tunnels.

For example, remote accessing VPN users should send DHCP request packets, but must not send any DHCP response packets for stability of the Ethernet segment. Another example is that the system administrator wants to detect and drop any ARP-poisoning packets due to security reason. Such demands cannot fulfilled by only packet filtering. Therefore, SoftEther VPN Server has a good security policy functions.

A security policy is the list of settings of values which determines whether particular harmful packet can be passed or must be discarded as follows. A security policy can be applied on both user object and group object on the VPN Server.

ss3.8.jpg

Security Policy can be set on either User Object or Group Object.

Filtering Harmful DHCP Packets

Via VPN Tunnel, any user can post harmful DHCP packets into the Ethernet segment by default. If a user sends a malicious and fake DHCP response packet to network where another user is waiting the DHCP response to determine his IP address, then the requesting user will take a wrong IP address. This will confuse the entire network. Then a security policy can restrict the type of DHCP packets which a user can send.

DHCP Spoofing and IP Addressing Enforcement

You can find some Ethernet switch produces on the contemporary market have DHCP spoofing functions in order to enforce a client computer to be assigned only the IP address which the DHCP server appointed. SoftEther VPN's Virtual Hub implements the exactly same features on it.

Prohibiting any Behavior as Bridges and Routers on VPN User's Side

Due to the character that SoftEther VPN Tunnel is fully virtualized layer-2 Ethernet network cable, then the remote-accessing VPN user can set up the router or the bridge on the user's side. It is easy for well-skilled users, in their home. It is not a good situation that any kidding users on their home can do some mischief with the VPN Session to the company's LAN. So a security policy can restrict any behavior as bridging or routing on the VPN Client side.

Prohibiting any Packets with Overlapped MAC Address and IP Address

If a user has IP address (for example, 192.168.3.2) and another user has the same IP address on the single Ethernet segment, it will be troublesome. Not only trouble, it also might be a risk of security because incorrect user can have an IP address and also can send an IP address imposing the correct one. So this type of behavior must be forbidden. This security policy can do it, not only for IP addresses, but also MAC addresses.

Reducing Broadcast Packets

If several hundreds of computers are connected on the single Ethernet segment via VPN, the number of broadcast packets will be increased by default. In such a case, turn this policy on to block all broadcast packets except ARP, DHCP and ICMPv6.

Privacy Filter Mode

A user which is set by this policy cannot communicate any other user who is set by this policy too. This policy is convenient the situation that the administrator allows users to access to only the central servers, but disallow to users to communicate each other, for security reason.

Preventing MAC and IP Address Table Flooding Attacks

A Virtual Hub on the VPN Server has FDB of MAC addresses. It also has IP Address tables. But some malicious VPN Client users might send random MAC addresses or IP addresses in source field of packets for the purpose to DoS attack (denial-of-service attack). It will consume the precious resource of VPN Server, especially the capacity of RAM. So use this security policy to limit the maximum numbers of both MAC Address and IP Address which is related on a user's VPN Session.

Bandwidth Limitation

Bandwidth Limitation can be applied on a VPN Session with a unit of bps (bits per seconds) to saving the entire bandwidth to the Internet. Both uploading (client-to-server) and downloading (server-to-client) can be specified separately as limitation value.

Limitation of Concurrent Multiple Logins of a User

By default, a user can connect to the VPN Server with multi VPN sessions concurrently. But you can restrict the maximum number of concurrent logins per a user by this security policy.

IPv6 Security Policy

You can also restrict the behavior of a user via VPN who is sending IPv6 packets. There are several new concepts in IPv6 than IPv4, then specific security policy dedicated for IPv6 is necessary. SoftEther VPN Server has fully functioned for IPv6 security enforcement.

3.9. Packet Monitor on VPN Session

Monitoring Function is a tapping function for all packets which are flowed in the Virtual Hub. This function can be used by network administrators of its VPN network. So this function is disabled by default, although an administrator can enable it if he wishes.

Monitoring Function is used from VPN Client with Ethernet tapping software, such as Wireshark, Ethereal, tcpdump or IDS (e.g. snort).

For Troubleshooting Purpose

You can use the monitoring function for troubleshooting purpose, because you can capture and analyze any packets flown in the VPN Server.

For IDS Purpose

You can use any kind of IDS (Intrusion Detection System) in order to detect potential security breaches on the network. You can attach IDS software to the VPN Server's Virtual Hub with the monitoring function.

ss3.9.jpg

Use Wireshark, tcpdump, snort or other analyzers to monitor all packets via Virtual Hub.

3.10. Packet Logger

All packets which are flowed via the Virtual Hub on the Virtual Server can be logged as a log file on the hard disk of VPN Server. But if you log all packets to record on the disk, the disk will be full soon. Then SoftEther VPN Server has a filtering function to determine what kind of packets is to be logged. And you can choose whether entire packet's payloads must be logged, or only important headers of packets must be logged. Due to processing by software, all packets will be logged without missing.

This function is usable not only troubleshooting, but also as evidence for such a case if a user will do some illegal actions against the company. Enabling the logging allows you to monitor all communications between the file server and database server from employees via VPN.

ss3.10.jpg

Packet Logging settings screen.

3.11. HTTP URL Logger

The HTTP-based traffic will be "deep-analyzed" for the HTTP header. Each target URLs on the HTTP connection request packets will be logged on the packet-logging file with plaintext of destination URLs. The system administrator can keep the HTTP access logs of employees who are using VPN Server, in order to audit the usage of VPN Server.

ss3.11.jpg

An example of Packet Log.
You can see headers of Ethernet, IP, TCP/UDP packet header values, and HTTP request headers.

3.12. Virtual Hub Admin Delegation

A VPN Server can have a lot of Virtual Hubs. And the administrator of the entire of VPN Server can entrust someone as an appropriate administrator of a Virtual Hub, and can delegate the role of it to him.

In this situation, the entire VPN Server's administrator specifies the administration password for dedicated to particular Virtual Hub, and tells that password to someone to delegate. Then delegated person can access and manage the Virtual Hub. But he still can't manage other Virtual Hubs on the same server. Security functions and databases such as for user objects and packet filter rules are separated between Virtual Hubs completely.

3.13. High Available and Stable Background Program

SoftEther VPN Server service was supposed to be running constantly and continuously 24h / 365d permanently after once VPN Server process has been started. Very careful efforts have been spent to develop the code sets of SoftEther VPN Server, especially preventing memory leaks and possibilities crashes. Currently released SoftEther VPN Server programs are believed that there are no vital bugs.

However, if something trouble happened on the process of SoftEther VPN Server, it will be restarted automatically. To prevent the loss of configuration data, all configuration data and statistics about the VPN session will be saved on the disk automatically with regular period. If a process stops suddenly, then the recovery task will be automatically invoked and it will restore the last states as possible.