1.5 Strong Security Features

Offering sufficient security is one of the most important matters for SoftEther VPN software designed and developed for the purpose of supporting backbone communication by company network, etc. Compared with older VPN solutions, SoftEther VPN software has new advanced security functions and offers sufficient security for VPN construction that can withstand the backbone work of businesses from small scale VPN. This section contains a description of the security functions that is offered by SoftEther VPN.

1.5.1 Abundant User Authentication Options

The types of user authentication when connecting SoftEther VPN Client or SoftEther VPN Bridge by VPN to SoftEther VPN Server include all sorts of methods as well as simple password database. All types of user authentication and parameters can be set in details for each user. Because the user database is managed separately for each Virtual Hub, Virtual Hubs are independent of each other.

User authentication methods that can be used will include the following. For details see 2.2 User Authentication.

- **Anonymous authentication**
  Anonymous authentication allows connection as long as at least the user name is known, and is used when establishing widely offered Virtual Hub service, etc. It is not usually used for businesses, etc.
- **Password Authentication**
  Standard password authentication is the method of conducting user authentication by user name and password. Also it is the method for which security that can be most easily maintained. Users can also change the password themselves by using VPN Client. The password is hashed when typed in so the password confirmation is conducted by challenge and it responses when authenticating, the password and hash data do not flow on the network.
- **RADIUS server authentication**
  Method of user authentication using RADIUS authentication server is already owned by company, etc.
- **NT domain and Active Directory authentication**
  Method of user authentication using Windows NT main controller or Active Directory of user database of Windows Server is already owned by company, etc.
- **Certificate authentication (PKI authentication)**
  Method of user authentication whereby those are connected to VPN is identified by mathematically calculating whether or not, those connection have a private key. By having those connection to VPN present a client can certificate to VPN Server. Because a fixed character string such as password is not used,we believe this is the most secure method of user authentication.

1.5.2 Robust Encryption

With SoftEther VPN protocol, all communication contents and data related to user authentication is encrypted by Secure Socket Layer (SSL) encryption. SSL is currently the standard security protocol for the Internet, and is used for communication between HTTP server and web browser (called "HTTPS protocol").

There are several versions of SSL, but SoftEther VPN supports SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.

SSL primarily offers three functions: encryption, electronic signature, and certificate authentication. All three of these functions are utilized for SoftEther VPN to maintain security of VPN sessions between SoftEther VPN Server and VPN connection source.

With the SSL implemented for SoftEther VPN algorithms used for encryption and those used for electronic signature are not fixed; the VPN Server administrator can choose the algorithm. The AES 128 bit encryption algorithm and SHA-1 hash algorithm are selected by default, but algorithms such as DES, RC4, or MD5 can be selected with specifying the number of bits.

Robust VPN session encryption by various encryption algorithms.

1.5.3 Server Certificate Verification

Many older VPN protocols have a user authentication function to identify and authenticate connection source users that have connected to the VPN server. Oppositely the majority of VPN clients have no function to confirm whether or not the VPN server that they are about to connect to will be authentic.

If you are constructing VPN by using a public IP network such as the Internet, however, there is the possibility of a malicious cracker, etc., lurking somewhere in the line setting up a false VPN server and relaying VPN communication from the client, reading or

tampering with the packets flowing through the VPN by "man-in-the-middle" (MITM) attack.

Commonly used protocols such as HTTPS and SSH check the certificate of the connection destination web server and SSH server and connect only if the certificate is authentic. when the certificate is not authentic, the connection is interrupted and a warning will be displayed. VPN communications requires a way to authenticate the connection destination server to guard against masquerading or MITM attack.

The server certificate presented by the connection destination server that can be trusted, and SoftEther VPN can make sure the server has the RSA private key for the secret by mathematical calculation. If the connection destination VPN Server presents a suspicious certificate, the VPN connection to the server is interrupted and a warning will be displayed. SoftEther VPN keeps a list of certificates that can be trusted. Certificates that is not signed by a reliable certification institution are regarded as untrustworthy (the user can keep a list of certificates).

Server certificate verification is conducted by the connection source software side, such as cascade connected VPN Server or VPN Bridge or VPN Client connected to remote VPN Server by usual method. For details on server certificate verification, see 4.4 Making Connection to VPN Server, etc.

1-5-2.png

Verifying server certificate presented by VPN Server.

1.5.4 Use with Smart Cards

When you are conducting user and are going to authenticate for VPN connection to VPN Server, if the password authentication or conventional certificate authentication is used, a certain degree of security can be maintained, but the following problems will be also existed.

- If you are using password authentication, or if your password in not long or complicated enough, there is danger of the password that can be guessed for unauthorized access. If a third party obtains a password from a second party that could observe the password being input, there will be a danger of unauthorized access by the third party.
- Certificate authentication provides a method of authentication that is more secure than password protection, but under ordinary circumstances, private key data of the certificate is kept in the hard disk of the computer. If the computer's hard disk is stolen by a malicious third party or only the certificate data is extracted, the third party can masquerade as the user using the private key data of the certificate and will be able to connect to the VPN server.

With SoftEther VPN, the certificate authentication is used to authenticate users when VPN Client connects to the VPN Server, because the certificate and private key data are written in a smart card or other hardware security token devices, instead of saving on the computer hard disk, the user authentication can be carried out by inputting each time the client connects to VPN Server.

Smart cards or other hardware security token devices have a built-in chip that performs RSA calculation, and electronic signature can be accomplished by using certificate and private key from the memory of the smart card without exposing the private key externally. Also with SoftEther VPN, existing certificates and private key objects stored are in smart cards can also be specified and used for user authentication.

Smart cards and other hardware security token devices are designed to be as once private key data is written inside, it cannot be extracted. The data in smart cards is protected by a PIN code consisting of several digits. Smart cards are designed to be as the smart card itself halts access if the PIN code doesn't match. Because of this protection, the private key can be loaded into the smart card, and by conducting user authentication using the private key in the smart card when you connect to the VPN Server, even if the computer itself or smart card has been lost or stolen, a malicious third party can be prevented from access by masquerading.

For information on how to use the user authentication function using a smart card, see 4.6 Using and Managing Smart Cards.

1-5-3.png

Smart card authentication.

See Also

- 2.2 User Authentication
- 2.2.1 Anonymous Authentication
- 2.2.2 Password Authentication
- 2.2.3 RADIUS Authentication
- 2.2.4 NT Domain and Active Directory Authentication
- 2.2.5 Individual Certificate Authentication
- 2.2.6 Signed Certificate Authentication
- 4.4 Making Connection to VPN Server
- 4.6 Using and Managing Smart Cards