2.3 Server Authentication

This section contains a description of the method of authenticating VPN client computers that connect to the SoftEther VPN Server in the previous item 2.2 User Authentication. Server authentication is oppositely the function whereby the VPN Server verifies that the VPN client computer (VPN client or VPN Server / VPN Bridge that conducts cascade connection) that attempts to connect to the SoftEther VPN Server is authentic. Normaly this function is off by default. Although server authentication is not needed for conventional operation, it can be enabled for each client connection setting or cascade connection setting.

2.3.1 Necessity of Server Authentication

Concerning Man in the Middle Attack in Internet of Public IP Network

Server authentication is needed when verifying whether the connection destination VPN Server when connecting to insecure VPN using public network is authentic. By planting special software that rewrites protocol in the line of an IP network, a malicious third party can technically make it appear as though you are connecting to an authentic VPN server when you are actually attempting to connect to a phony one. By redirecting connection from the phony VPN Server to the VPN Server the user intends to connect to, a malicious third party can temporarily read and re-encrypt and send all the packets flowing in the VPN to their destination post so they can eavesdrop or tamper with VPN communication without the user being aware of it.

This is called "direct attack", "man in the middle attack" or "person in the middle attack". Because of the enormous amount of traffic on the backbone of the Internet, realistically speaking, it is difficult to install special software on the backbone to conduct these attacks, but such attacks have succeeded in parts of network branches where throughput is not so high.

The server authentication function is therefore used if you want to prevent data transmitted in VPN from being eavesdropped on or tampered with by such attacks.

Mechanism of Server Authentication by Certificate

Server authentication by certificate verifies that the connection destination VPN Server is authentic by verifying the certificate, the opposite role of client certificate authentication such as described in 2.2 User Authentication. The connection destination VPN Server possesses an X.509 certificate and corresponding private key data, and the VPN client computer (VPN client or VPN Server / VPN Bridge that conducts cascade connection) that attempts to connect to VPN Server determines if the connection destination VPN Server can be trusted by the contents of the certificate. Because an RSA algorithm is used

for verifying the certificate, the VPN Server must have a private key that corresponds to the certificate.

If the server fails verification or presents an expired certificate, the connection destination VPN Server is determined to be insufficiently reliable and VPN connection is interrupted.

The two methods by which the VPN client computer (VPN client or VPN Server / VPN Bridge that conducts cascade connection) can determine whether the certificate presented by the connection destination VPN Server can be trusted are as follows.

2.3.2 Server Individual Certificate Authentication

Server individual certificate authentication is an authentication method whereby the X.509 certificate of the connection destination VPN Server is registered for each connection setting to VPN Server and connection to the VPN Server continues only when the certificate presented by the VPN Server when connecting matches the certificated registered in advance perfectly, and if not the connection will be cut off.

This method can be used if the server certificate of the connection destination VPN Server is already possessed. The contents of the certificate are displayed on the window when you first attempt to connect to the connection destination VPN Server with the mode for enabling confirmation of server certificate by VPN Client on enabled, and a message is displayed asking if want to register as the server individual certificate. If the user selects "Yes", beginning from the next time he connects to the VPN Server, the certificate used to connect the first time can be used as the server individual certificate.

2.3.3 Server Signed Certificate Authentication

Server signed certificate authentication is the authentication method whereby the VPN client computer that conducts VPN connection has a list or reliable root certificates (or intermediate certificates) and connection is allowed to continue if the certificate presented by the connection destination VPN Server is signed by one of the trusted certificates.

If there are several VPN Servers in the company or if the number is expected to increase in the future the server certificate of each VPN Server is signed by the company root certificate and by establishing that to root certificate is reliable, clients that attempt to connect to these VPN Servers can determine the servers are authentic if the certificates they present are signed by the root certificate.

See Also

- 2.2 User Authentication
- 6.5.37 "AccountServerCertEnable": Enable VPN Connection Setting Server Certificate Verification Option
- 6.5.38 "AccountServerCertDisable": Disable VPN Connection Setting Server Certificate Verification Option
- 6.5.39 "AccountServerCertSet": Set Server Individual Certificate for VPN Connection Setting
- 6.5.40 "AccountServerCertDelete": Delete Server Individual Certificate for VPN Connection Setting
- 6.5.41 "AccountServerCertGet": Get Server Individual Certificate for VPN Connection Setting