# 2.2 User Authentication

With SoftEther VPN, security is ensured by conducting strict user authentication when a new VPN session attempts to connect to a Virtual Hub to prevent a security violation whereby an unauthorized third party could connect to a Virtual Hub without permission.

In order to conduct user authentication, the Virtual Hub administrator must create users for the SoftEther VPN Server in advance, select from among 6 types of user authentication and specify the required parameters.

A type of user authentication can be specified for each created user. For example you can easily make it where Mr. A and Mr. B can connect to VPN by password authentication but the communications contents are limited by security policy and access list, and Mr. C can only connect with stricter certificate authentication but limitations are lenient.

The is section contains a description of each type of user authentication.

## 2.2.1 Anonymous Authentication

Anonymous authentication is the simplest type of user authentication. If a user set by anonymous authentication exists for Virtual Hub, anyone who knows the user name can connect to the Virtual Hub and conduct VPN communication.

With SoftEther VPN, anonymous authentication does not offer much help for business networks, etc. Anonymous authentication should be used in the following cases.

- If providing Virtual Hub that anybody can connect to for public IP network such as the Internet.
- If creating Virtual Hub that does not require user authentication for VPN server in company LAN. Case where for example streaming video can be viewed if connected to Virtual Hub.

## 2.2.2 Password Authentication

Password authentication is the easiest way to use for identifying and authenticating users. A password is established for the user if using password authentication.

Users will be refused to be accessed, if the password doesn't match when they attempt to connect to VPN. Users can change the password registered in VPN Server themselves at any time using VPN Client. For details see 4.9 Other Functions.

The passwords for password authentication are registered in the configuration database of SoftEther VPN Server. At this time the password is hashed by hash function, so the original password no longer exists. When conducting password authentication, SoftEther VPN protocol checks passwords for user authentication by challenge and response authentication (digest authentication). At this time the original password is not transmitted on the network.

The drawbacks of password authentication are as follows.

- If there are few users, operation can be conducted with no problem, but if there are more than several hundred users, it takes effort to register/delete users. In such cases, RADIUS authentication, NT domain or Active Directory authentication is used.
- The password base authentication method is connected with weaknesses such as the possibility of the password being guessed. Certificate authentication is used if corporate security policy does not recommend the password base authentication method and higher security is required.




*Password authentication.*

## 2.2.3 RADIUS Authentication

Just as with password authentication, RADIUS authentication authenticates user name and password, but when doing so, the password is managed by authentication server that supports RADIUS protocol rather than by the SoftEther VPN Server. This enables user authentication using the existing company password database. If company employees change their passwords on the RADIUS server, it also applies to the password for SoftEther VPN connection, thereby enabling password unification.

**Authentication Using RADIUS Server**

There are software based and hardware based RADIUS servers (authentication server that supports RADIUS protocol), both of which are widely used. Thus companies and Internet service providers that have RADIUS based authentication service can conduct user authentication by RADIUS server.

If users set to use RADIUS authentication conduct user authentication, the authentication data sent by the user (encrypted by SSL) is sent from the SoftEther VPN Server to the RADIUS server set in advance. Users that pass user authentication by the RADIUS server are permitted by the SoftEther VPN Server to connect. In any other case, permission will be denied (if user authentication fails or if RADIUS server cannot be accessed).

If using RADIUS authentication, the IP address of the SoftEther VPN Server is registered on the RADIUS server side, and after a password called "shared secret" is decided, Virtual Hub settings are changed. The RADIUS server to be used can be set for each Virtual Hub, and security settings of Virtual Hubs are independent of each other. The following 3 items are required to set RADIUS server settings for a Virtual Hub.

- **Host name and IP address of RADIUS server to be used**
- **UDP port number of RADIUS server to be used**
- **Shared secret decided in advance**

This information can be obtained from the RADIUS server administrator. The RADIUS server to be used must be set to enable use of Password Authentication Protocol (PAP).

The server product name that the SoftEther VPN Server notifies the RADIUS server of is **"SoftEther VPN Server"**.

2-2-2.png

*RADIUS authentication.*

**RADIUS Settings for Each User and for All Users**

If users within a Virtual Hub are authenticated by the RADIUS server, there are the following 2 methods:

- **If you only want to use RADIUS authentication for some users registered in advance:**
  In this case users to use RADIUS authentication as the method of user authentication are created and RADIUS authentication is set as the authentication method for those users. Then when the user attempts to connect to Virtual Hub, the input authentication information is verified by the RADIUS server and access is either permitted or denied. Also, if the user name for the Virtual Hub and that of the RADIUS server differ, you can specify a user name (other name) for the RADIUS server.
- **If you want to make all users registered for in the RADIUS server to connect to Virtual Hub by RADIUS authentication:**
  To basically permit all users already registered in the RADIUS server and users whose connection to Virtual Hub is registered, the user account is created with an asterisk (*) as the user name. By setting the user type, no matter what user name

the connection is made under, the user name and authentication information are checked by RADIUS Server, and if it passes authentication, access to the Virtual Hub is permitted. With this method, if a user passes RADIUS authentication and connects to Virtual Hub, even if a user of that user name is not actually registered to Virtual Hub, user authentication is passed, and the security policy setting value asterisk (*) is used as the user setting value. In other words, the asterisk (*) user is used as a template for VPN sessions connected by that method. Also if you want to allow all users registered in the RADIUS server except a few to connect to VPN, you can create user of user name to be denied and set that user for RADIUS authentication, and by disabling access permission as security policy, you can make that user fail user authentication. Also, even if there are users registered as an asterisk (*) or other users registered in Virtual Hub, user authentication by explicitly registered user data is first attempted, and only if it fails, RADIUS authentication is conducted via asterisk (*) user.

### 2.2.4 NT Domain and Active Directory Authentication

NT domain and Active Directory authentication are methods whereby user name and password are authenticated, just like with password authentication, but passwords are managed by NT domain controller of a Windows NT 4.0 Server or later or an Active Directory controller of Windows Sever rather than SoftEther VPN Server. This enables user authentication using the existing company password database. If company employees change their passwords on the Windows domain, it also applies to the password for SoftEther VPN connection, thereby enabling password unification.

**Authentication Using NT Domain Controller or Active Directory Controller**

Windows domain by Windows Server is already widely used. Thus companies and Internet service providers that have Windows domain based authentication service can conduct user authentication by NT domain controller or Active Directory controller.

If users set to use NT domain controller or Active Directory controller authentication conduct user authentication, the authentication data sent by the user (encrypted by SSL) is sent from the SoftEther VPN Server to the NT domain controller or Active Directory controller. Users that pass user authentication by the NT domain controller or Active Directory controller are permitted by the SoftEther VPN Server to connect. In any other case, permission is denied (if user authentication fails or if NT domain controller or Active Directory controller cannot be accessed).

If using NT domain or Active Directory authentication, the SoftEther VPN Server must be made to participate in the Windows domain to be used. SoftEther VPN Servers participating in the Windows domain can conduct NT domain or Active Directory

authentication of users set for NT domain or Active Directory authentication without special setting.

| |
|---|
| In order to conduct NT domain or Active Directory authentication, the SoftEther VPN Server to conduct user authentication must be capable of running on Windows NT, with capable of participating in domain. SoftEther VPN Servers that run on Windows 98, Windows 98 Second Edition, Windows Millennium Edition or Linux, FreeBSD, Solaris or Macintosh OS X cannot conduct NT domain or Active Directory authentication. VPN Server cannot authenticate the NT domain or Active Directory. In this case, while authentication method is set to “NT domain” or “Active Directory” domain, authentication does not work. |

2-2-3.png

*NT domain or Active Directory authentication.*

**NT Domain Authentication Setting for Individual Users and for All Users**

If users within a Virtual Hub are authenticated by NT domain controller or Active Directory controller, there are the following 2 methods:

- **If you only want to use NT domain controller or Active Directory controller for some users registered in advance:**
  In this case, users to use NT domain or Active Directory authentication as user authentication method are created and NT domain or Active Directory authentication is set as the authentication method for those users. Then when the user attempts to connect to Virtual Hub, the input authentication information is verified by the NT domain controller or Active Directory controller and access is either permitted or denied. Also, if the user name for the Virtual Hub and that of the NT domain controller or Active Directory controller differ, you can specify a user name (other name) for the NT domain controller or Active Directory controller.
- **If you want to make all users registered in the NT domain controller or Active Directory controller to connect to Virtual Hub by NT domain or Active Directory authentication:**
  To basically permit all users already registered in the NT domain controller or Active Directory controller and users whose connection to Virtual Hub is registered, the user account is created with an asterisk (*) as the user name. By setting the user type, no matter what user name the connection is made under, the user name and authentication information are checked by the NT domain controller or Active Directory controller, and if it passes authentication, access to the Virtual Hub is permitted. With this method, if a user passes NT domain or Active Directory authentication and connects to Virtual Hub, even if a user of that user name is not actually registered to Virtual Hub, user authentication is passed, and the security policy setting value asterisk (*) is used as the user setting value. In other words, the asterisk (*) user is used as a template for VPN sessions connected by that method. Also if you want to allow all users registered in the NT domain controller or Active Directory controller except a few to connect to VPN, you can create user of user name to be denied and set that user for NT domain or Active Directory authentication, and by disabling access permission as security policy, you can make that user fail user authentication. Also, even if there are users registered as an asterisk (*) or other users registered in Virtual Hub, user authentication by explicitly registered user data is first attempted, and only if it fails, NT domain or Active Directory authentication is conducted via asterisk (*) user.

## 2.2.5 Individual Certificate Authentication

### Matters Common to Certificate Authentication

With password authentication, RADIUS authentication, NT domain and Active Directory authentication, user authentication is accomplished by the VPN client side proving that it is authorized to connect to the SoftEther VPN Server by user name and password. The method of user authentication using passwords generally offers sufficient security, but if corporate security policy does not recommend using a password for user authentication,

user authentication must be conducted using a more secure method called certificate authentication (also called PKI authentication). There are 2 kinds of certificate authentication -- individual certificate authentication and signed certificate authentication. Each user may select the kind that best suits his needs. The SoftEther VPN Client that attempts to connect to the SoftEther VPN Server in the client certificate authentication mode can select either the client computer's hard disk or an external smart card as the place for storing the certificate and private key.

With certificate authentication, when the connection source computer attempts to connect to the Virtual Hub it presents a user name together with an X.509 electronic certificate. The SoftEther VPN Server checks whether is correct and the connection source computer is only allowed to connect if it passes.

The connection source computer must possess certificate data and a private key (RSA private key) that corresponds to the public key in the certificate to present. Certificate data is sent from the connection source computer to the VPN Server by private key data is not transmitted. Next the VPN Server sends random number data (called challenge values) to the client. When the client receives the data, it signs it by the private key it possesses and returns the data. VPN Server verifies the signature data sent by the client using the public key in the electronic certificate initially received and makes sure that the client computer has the certificate and corresponding private key (if it can't be confirmed, user authentication fails on the spot). It subsequently checks if the certificate subsequently presented by the client matches the attributed defined for each user as user authentication data. You can select either individual certificate authentication or signed certificate authentication as the test method at this time.

| |
|---|
| Certificates that can be used with SoftEther VPN are X.509 format. RSA is used for PKI algorithm, and bit length for public and private keys is 1,024 or 2,048 bits. Version 1 of X.509 certificates and later can be used, but some extension fields are not supported (contents are ignored). The subject values that can be recognized by all SoftEther VPN modules are "CN" and "O" and "OU", "C" and "ST", "L". |

Certificates which have expired and those registered in the list of invalid certificates that can be set per Virtual Hub are recognized as invalid and user authentication always fails.

2-2-4.png

*Certificate authentication.*

**Client Certificate Authentication by Individual Certificate Authentication**

With individual certificate authentication, certificate data is registered for user in Virtual Hub side user database, and permission to connect is granted if the certificate presented by the user perfectly matches the previously registered certificate.

**Advantages of Individual Certificate uthentication**

Using individual certificate authentication facilitates use of SoftEther VPN with certificate authentication function. Especially if the number of users using certificate authentication ranges from several users to tens of users, the VPN system can be operated sufficiently by individual certificate authentication. As for the specific operation method, the Virtual Hub administrator creates several X.509 certificates, registers them sequentially in the Virtual Hub, and by transferring the certificate and private key to the user by a secure method (e-mail in company LAN, shared folder or smart card), the user can use them to connect to Virtual Hub of VPN Server any time. Oppositely the user can create the certificate and can register it by transferring to the Virtual Hub administrator (this method is more secure because the private key never leaves from the user's possession).

The private key and X.509 certificate can be created with a utility (freeware or commercially available software) that supports various existing PKIs. The X.509

certificate file and private key file can be created by the MakeCert command of certificate creation tool and SoftEther VPN command line management utility (vpncmd) which are functions of SoftEther VPN Server Manager (see 6. Command Line Management Utility Manual). These simple utilities support creation of both self-signing certificates and signed certificates.

**Disadvantages of Individual Certificate Authentication**

individual certificate authentication is difficult to use if there a large number of users that need to be registered or PKI has been adopted by the company and each employee has a private key in a smart card (employee ID, etc.). In such a case we recommend you select signed certificate authentication.

## 2.2.6 Signed Certificate Authentication

**Client Certificate Authentication by Signed Certificate Authentication**

Signed certificate authentication is convenient when used when company CA (Certification Association) distributes X.509 certificate and private key file to each individual employee. Also if PKI system is currently not yet adopted but you want to allow a large number of users to access Virtual Hub, it can be used if you want to use certificate authentication. The requirements for using this method are as follows.

- An X.509 certificate and corresponding private key must be distributed to each user to access Virtual Hub by file or smart card.
- Certificates for each respective user are signed by root certificate (or intermediate certificate) and private key possessed by company CA (certificate association) and have tree structure reliability relationship.

If using signed certificate authentication, root certificate (or intermediate certificate) signed for each user is registered in the certificate list of CA trusted by Virtual Hub.

Next, new user is created and signed certificate authentication is set as the authentication method for that user. Thus if the certificate presented by client computer connected by user name is confirmed to be signed by a certificate the certificate list of a trusted CA registered in Virtual Hub, that client computer passes user authentication.

With this method, however, because of equal treatment, any employee having a certificate issued by company root CA for example if users who want to increase the types of protocol that can be communicated are differentiated, it is used together with method of limiting connectable certificates by serial number or Common Name, which will be described next.

**Limit of Connectable Certificate by Common Name or Serial Number**

The contents of X.509 certificate may include Common Name (CN) and serial number. In such case, by limiting Common Name and serial number, for example, even in the case where it could not be confirmed that the certificate is signed by a certificate of a CA trusted Virtual Hub or when one or both items of the serial number do not match perfectly, access can be denied.

If this function is used, by creating users that can connect only if certain serial number or CN value of certificate signed by certificate that can be trusted, security policy, etc. can be differentiated according to type of certificate.