3.5 Virtual Hub Security Features

This section explains the Virtual Hub security functions, methods for their setting and important points to be aware of.

3.5.1 Delegating Virtual Hub Administration Authority

Entire VPN Server Administrators & Virtual Hub Administrators

Administrators of the entire SoftEther VPN can set passwords for Virtual Hubs and delegate the authority for their individual administration to Virtual Hub Administrators.

The Virtual Hub Administrators are then required to use the Virtual Hub name and password which they are assigned to connect to the VPN. Moreover, the areas which can be administered are limited by their own Virtual Hub's settings, which cannot be enabled to obtain information on other Virtual Hubs.

While individual Virtual Hub Administrators may view the settings of the entire VPN Server, they are not able to change them. Furthermore, no access whatsoever is possible to data containing confidential items such as the VPN Server's Configuration file and SSL Certificate private key file.

Virtual Hub Administrator Authority

Administrators to whom the administration of a Virtual Hub has been delegated can change their own administration password at any time. They can also change the Virtual Hub's online / offline status at any time. In addition, it is also possible to change various settings relating to the Virtual Hub, create cascade connections and define user and group objects. However, these settings changes may become subject to limitations imposed by the entire VPN Server Administrator. Please refer to 3.5.12 for details on how the VPN Server Administrator can restrict the contents of tasks which can be performed by the Virtual Hub Administrators.

Note that the Virtual Hub Administrator cannot alter that Virtual Hub's type (Static/ Dynamic) in a clustering environment, and this setting can only be changed by the entire VPN Server Administrator.

3.5.2 Virtual Hub Anonymous Enumeration Settings

Entering the host name and port number of the destination VPN Server in the Windows version SoftEther VPN Client Manager or VPN Server Manager automatically acquires a

list of the Virtual Hubs registered on that VPN Server and displays them in a drop-down list box. This is known as "Virtual Hub anonymous enumeration", which indicates that it is possible to enumerate a list of Virtual Hubs registered on an anonymously-designated VPN Server even if the user is not actually logged onto the VPN Server.

3-5-1.png

Virtual Hub anonymous enumeration.

However, some Virtual Hub Administrators may not wish for the name of the Virtual Hub which they administer to be able to be seen by anonymous users. In this case, opening the [Security settings] box in the [Virtual Hub properties] with the VPN Server Manager and enabling the [Don't Enumerate This Hub for Anonymous Users] checkbox prevents the Virtual Hub name from being displayed on the VPN Server Virtual Hub list enumerated by anonymous users.

The same task can be performed in the vpncmd utility using the command **[SetEnumDeny]**.

3-5-2.png

Disable enumeration for anonymous users setting.

Carrying out this setting means that a Virtual Hub for which the [Do not enumerate this Virtual Hub to anonymous users] checkbox is enabled is also no longer displayed to other individual Virtual Hub Administrator users who are neither entire VPN Server Administrators nor the Administrators of that Virtual Hub, when they acquire a list of Virtual Hubs registered on the VPN Server using either the initial Virtual Hub list window in the VPN Server Manager or the **[HubList]** command in the vpncmd utility. In other words, users who are not aware of the existence of that Virtual Hub are not even able to view the hub's name. This is effective when the name of the Virtual Hub itself has a meaning which the Administrator wishes not to disclose.

3.5.3 External Authentication Server Settings

Virtual Hub Administrators wishing to authenticate users with RADIUS authentication need to set the RADIUS server to be used in advance and this can be done by clicking the [Authentication server settings] button. In the vpncmd utility, this setting can be made using **[RADIUSServerSet]** command.

Please refer to 2.2 User Authentication for details on the items which need to be set. There is no need to perform domain controller settings when using NT domain or Active Directory authentication.

3-5-3.png

RADIUS server settings window.

3.5.4 Users and Groups

Users and Groups

A plurality of users and groups can be registered on a Virtual Hub. Users are able to not participate in groups or to participate in only one group. A single user cannot participate in two or more groups at the same time.

Groups administer a collection of multiple users and are useful when wishing to apply the same security policies to all users registered in that group.

Deleting a group causes all users participating in that group to cease to belong to any group.

To display a list of users with the VPN Server Manager, click on the [Manage Users] button. To display a list of groups, click on the [Manage Groups] button. Administration of users and groups is carried out on the windows displayed by clicking these buttons. A list of registered users and groups can be obtained using the vpncmd utility with the **[UserList]** and **[GroupList]** commands respectively.

User List

Opening the [Manage Users] window with the VPN Server Manager or calling up the **[UserList]** command with the vpncmd utility displays a list of users registered on the Virtual Hub. In addition to the user's name, their actual name, group to which they are attached, description, selected user authentication method, number of logins to date and most recent login time & date are also displayed.

3-5-4.png

Manage Users window.

Creating Users

Click on the [Create] button in the VPN Server Manager to create a new user. In the vpncmd utility, use the **[UserCreate]** command.

When creating a new user, it is necessary to decide on a user name. Alphanumeric characters and some symbols can be used for user names but special names used internally by the VPN Server cannot be designated (designating these names causes an incorrect parameter error). Arbitrary characters can be designated for the [Real name] and [Description] entry columns because they are not related to operation of the VPN Server. The items set when creating a new user can be changed at a later date.

An [Expiration date] can also be set for user objects. Users on whom an expiration date has been set are no longer able to connect to the VPN Server after said date.

3-5-5.png

User create & edit window.

Authenticating Users

User authentication methods have to be selected. Please refer to for details on each method. At the same time, parameters corresponding to the authentication method must also be designated. These parameters can be set simply with the GUI in the VPN Server Manager, while the same tasks can be carried out in the vpncmd utility using the **[UserAnonymousSet]**, **[UserPasswordSet]**, **[UserCertSet]**, **[UserSignedSet]**, **[UserRADIUSSet]** and **[UserNTLMSet]** commands.

Certificate Create Tool

The window in the VPN Server Manager tool for creating new users and editing user information contains a [Create Certificate] button. This tool enables the simple generation of an X.509 Certificate and private key pair.

Displaying User Information

Statistical information on each user can be obtained. Select the user with the VPN Server Manager and click on the [View user Info] button. In the vpncmd utility, use the **[UserGet]** command.

The user information includes the time & date on which the user object was created, time of last update and number of logins as well as statistical information on network communication.

3-5-6.png

User information window.

Group List

Opening the [Manage Groups] window with the VPN Server Manager or executing the **[GroupList]** command with the vpncmd utility displays a list of groups registered on the Virtual Hub. In addition to each group's name, their actual name, description and number of participating users are also displayed.

3-5-7.png

Manage Groups window.

Creating and Editing Groups

To create a new group, click on the [Create new] button in the [Manage Groups] window of the VPN Server Manager. To edit the information of an existing group, click the [Edit] button. In the vpncmd utility, the **[GroupCreate]** and **[GroupSet]** commands can be used.

3-5-8.png

Creating and Editing a Group window.

Adding Users to a Group

To add a user to a group using the VPN Server Manager, enter the name of the group to which the user is to be attached in the [Group name] box of the user information edit window or select from the list in [Browse Groups]. When deleting a user from a group, leave the [Group name] box blank. In the vpncmd utility, the **[GroupJoin]** and **[GroupUnjoin]** commands can be used.

Displaying Group Information

When there are users participating in a group, the VPN Server also records statistical information on the communication volume for that group when communication occurs in a VPN session connected by its users. To view this information, open the desired group's edit window in the VPN Server Manager and select [Statistical information of this group]. In the vpncmd utility, use the **[GroupGet]** command.

3.5.5 Trusted Certification Authority Certificates

A list of the trusted certification authority certificates can be administered on the Virtual Hub. This certificate list can be used for the functions in 3.4.12, in addition to its use for checking whether the certificate submitted by a user is trusted by signed certificate authentication in user authentication (2.2 User Authentication).

To register or delete a CA certificate trusted by a Virtual Hub, click on the [Trusted CA Certificate] button in the VPN Server Manager and select [Add] or [Delete] or click the [View Certificate] button. In the vpncmd utility, use the **[CAList]**, **[CAAdd]**, **[CADelete]** and **[CAGet]** commands.

3-5-9.png

Manage Trusted CA certificate window.

3.5.6 Certificates Revocation List

Role of the Certificates Revocation List

A list of disabled certificates can be administered on the Virtual Hub. An invalid certificate definition has priority over a trusted CA certificate definition. When one of several certificates issued by a root certification authority is compromised or the user of that certificate resigns the company and so on, this function can be used to forcibly disable the certificate on the server side by registering its serial number and other details.

When a user submits a certificate which matches the conditions registered on the Certificates Revocation List, user authentication is denied even if that certificate was signed by a certificate registered in the trusted CA certificates list.

Adding to, Deleting & Editing the Certificates Revocation List

To add a new definition to a Virtual Hub's disabled certificates list, or to edit or delete an existing definition, click on the [Invalid Certificate] button in the VPN Server Manager

and click either the [Add], [Delete] or [Edit] button. In the vpncmd utility, use the **[CrlList]**, **[CrlAdd]**, **[CrlDel]** and **[CrlGet]** commands.

3-5-11.png

Certificates Revocation List window.

Registering Certificates Revocation Data

In order to define a new disabled certificate, it is necessary to designate that certificate's subject field values, its serial number and MD5 or SHA-1 digest values. In addition, when the certificate to be disabled has an X.509 file, it is also possible to disable the certificate by having it read from the VPN Server Manager.

For data registered as a disabled certificate, certificates matching all of the contents of the defined items are disabled. If the serial number and digest values of the certificate to be disabled are already known, it is possible to disable only that certificate with a high degree of certainty by inserting this information. For all other cases, designating the CN / O / OU / C / ST / L subject field values and performing filtering then disabling those certificates caught by the filter is an effective measure.

When the connection from a VPN Client using the certificate to be disabled has been successful to date, the subject fields, serial number and digest values of the certificate submitted by the user when successfully authenticated are recorded in the Virtual Hub security log and the VPN Server's server log, so carrying out the disable settings based on this information is an assured method.

3.5.7 Setting CN & Serial Number on Signed Certificate Authentication

When the authentication type of a user registered on the Virtual Hub is signed certificate authorization, it is possible to allow connection only when the CN (Common Name) and serial number of the X.509 certificate submitted by the user are examined and found to match completely the predefined user object setting values. Please refer to section 2.2 User Authentication entitled [Limit of connectable certificate by Common Name or serial number].

3.5.8 Setting an Alias in RADIUS Authentication or NT Domain & Active Directory Authentication

It is possible to designate an alias for the user name registered as the Virtual Hub user object during RADIUS authentication or NT Domain & Active Directory authentication, and carry out user authentication using this alias by requesting authentication from the RADIUS authentication server and domain controller. For details, please refer to 2.2 User Authentication.

3.5.9 Security Policies

Definition of Security Policy

The security policy function is one of the SoftEther VPN Server Virtual Hub's sophisticated functions which allows only packets which have passed packet content inspection and policies to pass. In applying a security policy, the Virtual Hub interprets the header information of all virtual Ethernet frames flowing over it internally to a high layer (automatic recognition of ARP / IP / TCP / UDP / ICMP / DHCP etc) and determines whether their communication content conforms to a security policy based on the results of that interpretation. As a result, any virtual Ethernet frames which breach the security policies set for users by the Virtual Hub Administrator are discarded. In addition, these security policy violations are, depending on their contents, recorded in the Virtual Hub's security log where they can later be inspected by the Virtual Hub Administrator.

Utilizing security policies also enables detailed VPN communication control such as band control.

Sequence for Applying Security Policies

Security policies can be set for users who can be defined on the Virtual Hub. Where a plurality of users are grouped together, security policies can also be applied to the group. The decision on what type of security policies will be applied to a session when a VPN

connection is made to a Virtual Hub is decided automatically by the VPN Server. The order of priority in determining this application is as follows.

1. When security policies are set for a user attempting to connect to the VPN, those settings is adopted.
2. When security policies are not set for a user attempting to connect to the VPN and that user belongs to a group, the security policies set for that group are applied to the user.
3. Where the user is the Administrator in 3.4 Virtual Hub Functions, special Administrator security policies are set.
4. For all other scenarios, the default security policies (see next section) are applied.

Default Security Policies

The default security policy values are as follows.

- [Allow access] is enabled
- [Maximum Number of TCP connections] is 32
- [Time-out Period] is 20 seconds

Setting Security Policies for Users & Groups

To apply security policy settings to user objects or group objects using the VPN Server Manager, enable [Set Security Policy] checkboxes in the user or group edit window, then click the [Security Policy] button and edit as desired.

3-5-12.png

User & group security policy edit window.

List of Security Policy Items

The SoftEther VPN Server's security policy settings have the following 20 policy items which can be modified.

Allow Access policy	
Description	Users for whom this policy is set are allowed to make a VPN connection to the VPN Server.
Settable Values	[Enabled] and [Disabled]
Default Values	[Enabled]
Remarks	This security policy cannot be designated together with the connection settings of a cascade connection.
Filter DHCP Packets policy	
Description	Filters all DHCP packets in sessions for which this policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None
Deny DHCP Server Operation policy	

Description	Forbids the computer connected to sessions for which this policy is set from acting as a DHCP Server and distributing IP addresses to DHCP clients.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None
Enforce DHCP Allocated IP address policy	
Description	Prevents computers within sessions for which this policy is set from using any IP addresses other than those assigned by the DHCP Server on the virtual network.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None
Deny Bridge Operation policy	
Description	Denies bridge connections in user sessions for which this policy is set. Communication is not possible even if an Ethernet bridge is set up on the user's client side.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	This security policy cannot be designated together with the connection settings of a cascade connection. Note that sessions connected by users on whom both the deny bridge and deny router operation policies are [Enabled] cannot connect to the virtual hub as a [Router/ Bridge Mode] session. Contrarily, it is important to note that when either one or both of the deny bridge and deny router operation policies are [Disabled], the user is able connect to the virtual hub as a [Router/ Bridge Mode] session.
Deny Routing Operation policy	
Description	Denies IP routing in sessions for which this policy is set. Communication is not possible even if an IP router is operating on the user's client side.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	This security policy cannot be designated together with the connection settings of a cascade connection. Note that sessions connected by users on whom both the deny bridge and deny router operation policies are [Enabled] cannot connect to the virtual hub as a [Router/ Bridge Mode] session. Contrarily, it is important to note that when either one or both of the deny bridge and deny router operation policies are

	[Disabled], the user is able connect to the virtual hub as a [Router/ Bridge Mode] session.
Deny MAC Addresses Duplication policy	
Description	Prevents the use of MAC address tables currently in use by a computer in a separate session in sessions for which this policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None
Deny IP addresses Duplication policy	
Description	Prevents the use of MAC address tables currently in use by a computer in a separate session in sessions for which this policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None
Deny Non-ARP/ DHCP broadcasts policy	
Description	Denies the transmission and receipt of all broadcast packets on the virtual network other than ARP protocol and DHCP protocol broadcast packets in sessions for which this policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None
Privacy Filter Mode policy	
Description	Filters all direct intersession communication in sessions for which the Privacy Filter Mode policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	This security policy cannot be designated together with the connection settings of a cascade connection.
Deny Operation as TCP/IP server policy	
Description	Denies computers in sessions for which this policy is set from operating as servers in TCP/IP protocol. In other words, that session is unable to respond to a SYN packet in TCP from a separate session.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None
No limit on Number of Broadcasts policy	

Description	Does not automatically limit the number of broadcast packets sent to the virtual network from computers for which this policy is set, even if said number differs greatly from one which would be considered normal.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None
Allow Monitoring Mode policy	
Description	Allows users for whom this policy is set to connect to a virtual hub in Monitoring Mode. Monitoring Mode sessions can monitor (intercept) all packets flowing within the virtual hub.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	This security policy cannot be designated together with the connection settings of a cascade connection.
Maximum Number of TCP Connections policy	
Description	Sets the maximum number of TCP connections which can be assigned for each session in sessions for which this policy is set.
Settable Values	1 - 32 (connections)
Default Values	32 connections
Remarks	This security policy cannot be designated together with the connection settings of a cascade connection.
Time-out Period policy	
Description	Sets the timeout time in seconds until a session disconnects when a failure occurs in communication between the VPN Client and the VPN Server in sessions for which this policy is set.
Settable Values	5 - 60 (seconds)
Default Values	20 seconds
Remarks	This security policy cannot be designated together with the connection settings of a cascade connection.
Maximum Number of MAC Addresses policy	
Description	Sets the number of MAC addresses which can be registered per session in sessions for which this policy is set.
Settable Values	[No setting] or 1 - 65,535 (addresses)
Default Values	[No setting]
Remarks	None
Maximum Number of IP Addresses policy	
Description	Sets the number of IP addresses which can be registered per session in sessions for which this policy is set.

Settable Values	[No setting] or 1 - 65,535 (addresses)
Default Values	[No setting]
Remarks	None
Upload Bandwidth policy	
Description	Limits the bandwidth of external traffic entering the virtual hub in sessions for which this policy is set.
Settable Values	[No setting] or 1 - 4,294,967,295 bps (about 4 Gbps)
Default Values	[No setting]
Remarks	None
Download bandwidth policy	
Description	Limits the bandwidth of internal traffic leaving the virtual hub in sessions for which this policy is set.
Settable Values	[No setting] or 1 - 4,294,967,295 bps (about 4 Gbps)
Default Values	[No setting]
Remarks	None
Deny Changing Password policy	
Description	Denies users for whom this policy is set from changing their own password using the VPN Client Manager and so on at user password verification.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	There is no point in applying this policy to a group. In addition, this security policy cannot be designated together with the connection settings of a cascade connection.
Maximum Number of Multiple Logins policy	
Description	Denies users for whom this policy is set from performing more than a set number of simultaneous logins. This security policy can only be enabled in the VPN Server which features the multiple login limit function.
Settable Values	[No setting] or 1 - 65,535 (logins)
Default Values	[No setting]
Remarks	None
Deny VoIP / QoS Function policy	
Description	Denies use of VoIP / QoS response function in user VPN connection sessions for which this policy is set. This security policy can only be enabled in the VPN Server which features the VoIP / QoS response function.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Remarks	None

Confirming Contents of Applied Security Policies

Users are able to confirm the values of security policy settings applied to the current session when a VPN Client is connected to a VPN Server Virtual Hub. For details, please refer to 4.5 Connect to VPN Server.

3.5.10 Packet Filtering with the Access List

Role of the Access List

Up to 4,096 access list entries can be defined in a Virtual Hub. An access list is a function which either passes or discards IP packets passing through network devices according to designated rules commonly referred to as packet filtering rules.

3-5-13.png

Access list administration window.

Data which can be Defined by Access List Entries

The following data can be defined by the access list registered in the Virtual Hub.

- **Access List Memo**
  Enter a description of the access list entry. This entry enables the setting of an arbitrary character string to clarify the entry for the Virtual Hub Administrator, and its contents has no effect on packet filtering operation.

- **Action**
  Designates how an IP packet should be treated when a matching entry definition is found in the access list. Sets to [Pass] or [Discard].
- **Priority**
  Designates the priority of an entry within the access list as an integer. The lower the integer, the higher the priority. If there are access list entries with the same priority, it is undefined as to which is applied first.
- **Source IP address**
  Designates the sending IP address as the packet's matching criteria. It is also possible to designate a subnet range including multiple IP addresses by designating the network address and subnet mask. All sending IP addresses match when no range is designated.
- **Destination IP address**
  Designates the destination IP address as the packet's matching criteria. It is also possible to designate a subnet range including multiple IP addresses by designating the network address and subnet mask. All destination IP addresses match when no range is designated.
- **Protocol Type**
  Designates the protocol number of that IP packet as the packet's matching criteria. It is possible to match all IP protocols. The numbers which can be designated can be entered as integers although 6 (TCP/IP), 17 (UDP/IP) and 1 (ICMP) are already defined.
- **Source / destination port number range**
  Minimum or maximum source port and destination port numbers can be designated as the packet's matching criteria when TCP/IP or UDP/IP is selected as the protocol type. All port numbers are regarded as matching when no values are designated.
- **Source user name**
  A user name can be designated as the packet's matching criteria when wishing to match only those packets sent by a specific user (strictly speaking, it is the packet sent by the VPN session of a specific user name). Sending user names are not checked when no name is designated.
- **Destination user name**
  A user name can be designated as the packet's matching criteria when wishing to match only those packets to be received by a specific user (strictly speaking, it is the packet intended to be received by the VPN session of a specific user name). Destination user names are not checked when no name is designated.

When none of the Access List Entries Match

When multiple access lists are registered on a Virtual Hub and the IP packet does not match any of the entries contained therein, a [Pass] action is decided by default.

Adding, Deleting & Editing Access List Entries

To add, delete or edit entries in the access list, click on the [Manage Access lists] button in the VPN Server Manager. Next click on the [Add], [Delete] or [Edit] buttons. Be sure to click the [Save] button after completing any changes to the access list, as changes are not applied to the Virtual Hub unless saved. Furthermore, the access list is enabled from the instant it is set (also applies to VPN sessions which are already connected).

To modify the access list with the vpncmd utility, use the **[AccessAdd]**, **[AccessList]**, **[AccessDelete]**, **[AccessEnable]** and **[AccessDisable]** commands.

3-5-14.png

Access list entry edit window.

3.5.11 Limiting Connections with the IP Access Control List

IP Access Control List

Using the "IP access control list" makes it possible to allow or deny a VPN source computer attempting to make a VPN connection to a Virtual Hub depending on the computer's physical IP network address.

Although the "IP access control list" is similar to the "access list" in terms of its name and settings,these two are completely different. While the "access list" controls IP packets flowing in a Virtual Hub using their IP addresses, protocol port numbers and so on, the "IP access control list" is used to refine the physical IP addresses of connection sources which can make a VPN connection to the Virtual Hub.

This may involve, for instance, setting up a permanent cascade connection to the VPN server from the VPN Bridge of a separate hub when connecting company sites to the VPN. However, where security concerns exist, it is possible to set the "IP access control list" of the Virtual Hub receiving the VPN Server cascade connection to refuse any VPN connections to the Virtual Hub other than from the physical IP address of the site in which the VPN Bridge is set up. Put simply, it is possible to perform authentication based on the connection source's IP address. This significantly enhances security because it prevents connection source VPN client computers which are denied based on their source IP address from proceeding even to the user authentication phase.

IP Access Control List Rules

Multiple rules can be added to the "IP access control list", and the values which can be defined in these rules are as follows.

- **Source IP address** (single or subnet)
- **Action** (Permit connection / Deny Connection)
- **Priority** (Designate with integers. As is the case for access list entries, the lower the priority, the higher the integer.

Designating a source IP address of 0.0.0.0 / 0.0.0.0 enables the creation of rule entries to apply to all IP addresses.

Examples of IP Access Control List Settings

Create the following two entries when wishing to allow connections from the IP address 130.158.6.51, for instance, but deny all other IP addresses.

- **Entry with priority of 10**
  allows connections from IP address 130.158.6.51 (single host)
- **Entry with priority of 20**
  denies connections from IP address 0.0.0.0 subnet mask 0.0.0.0

Making this setting allows VPN connection requests with the source IP address 130.158.6.51 and enables it to proceed to the user authentication phase. Connection requests from sources with all other IP addresses are denied before the user authentication phase, so using the IP access control list can enhance security, particularly

when using Virtual Hubs in a site-to-site VPN where the source IP addresses and their ranges are known to a certain extent.

Adding, Deleting & Editing IP Access Control List Entries

To add, delete or edit entries in the IP Access Control List, first open [Virtual Hub properties] in the VPN Server Manager and click on the [IP Access Control List] button. Next click on the [Add Rule], [Edit Rule] or [Delete Rule] buttons. Be sure to click the [Save] button after completing any changes to the IP access control list, as changes are not applied to the Virtual Hub unless saved. The IP access control list is enabled from the instant it is set, but this does not mean that all of those sessions already connected to which the new changes are applied and which do not match the new rules are immediately disconnected.

The IP access control list can be operated in the vpncmd utility using the **[AcList]**, **[AcAdd]** and **[AcDel]** commands.

3-5-15.png

IP access control list window.

3.5.12 Virtual Hub Administration Options

Virtual Hub Administration Options

As explained in 3.5.1, Virtual Hub Administrators possess the authority to perform most settings on their own hub at their own discretion. However, there may be situations where some functions need to be disabled and made unavailable to the Virtual Hub Administrators such as disabling the cascading function from one Virtual Hub to another or disabling the SecureNAT function.

In these situations, using the Virtual Hub Administration Options enables the VPN Server Administrator to designate and control the details of the Virtual Hub Administrator's authority.

Virtual Hub Administration Option window.

Virtual Hub Administration Option Values

The Virtual Hub Administration Options entry list is composed of alphabetic characters (keywords) and their corresponding values. The initial value of a created hub is set at 0 for all entries. By setting this value as 1 or designating an arbitrary integer it is possible to restrict the authority that a Virtual Hub Administrator can exercise.

The names of the Virtual Hub administration options entries follow naming conventions.

Designate a value of 0 or 1 for entry names beginning with **"allow_", "deny_"** and **"no_"**. Designating 0 disables the restriction placed by that Virtual Hub administration options entry, whereas designating 1 enables it.

Designate a value of 0 or an arbitrary integer of 1 or more for entries beginning with **"max_"**. A value of 0 means no limitations, whereas a value of 1 or more restricts the maximum to that value.

The following Virtual Hub administration options are available on the SoftEther VPN Server versions at the time of writing.

- **allow_hub_admin_change_option**
  This entry is special in that a value of 1 (Enabled) allows not only the entire VPN Server Administrator but also the Virtual Hub Administrators to alter their own Virtual Hub administration options.
- **max_users**
  Designating a value of 1 or more for this entry restricts the maximum number of users which can be registered on the Virtual Hub, and no user objects beyond this value can be registered.
- **max_groups**
  Designating a value of 1 or more for this entry restricts the maximum number of groups which can be registered on the Virtual Hub, and no group objects beyond this value can be registered.
- **max_accesslists**
  Designating a value of 1 or more for this entry restricts the maximum number of access lists which can be registered on the Virtual Hub, and no access lists entries beyond this value can be registered.
- **max_sessions**
  Designating a value of 1 or more for this entry restricts the maximum number of VPN sessions which can be registered on the Virtual Hub, and any VPN connections beyond this value are unable to be simultaneously processed.
- **max_sessions_client**
  When the max_sessions_client_bridge_apply entry is 1 (Enabled), the number of client connection sessions which can be simultaneously connected to this Virtual Hub is not able to exceed the value set for max_sessions_client. The

max_sessions_client entry value is ignored when the max_sessions_client_bridge_apply entry is set at 0.

- **max_sessions_bridge**
  When the max_sessions_client_bridge_apply entry is 1 (Enabled), the number of bridge connection sessions which can be simultaneously connected to this Virtual Hub is not able to exceed the value set for max_sessions_bridge. The max_sessions_bridge entry value is ignored when the max_sessions_client_bridge_apply entry is set at 0.
- **max_sessions_client_bridge_apply**
  Only when this entry is 1 (Enabled) are the max_sessions_client and max_sessions_bridge entries meaningful.
- **max_bitrates_download**
  When this entry is set at 1 or more, the value of the [Download bandwidth] security policy is forcibly changed to this entry value and download speed is restricted for all VPN sessions connected to the Virtual Hub. For instance, setting this value at 1000000 means that all VPN connection sessions on this Virtual Hub are not able to exceed the download speed of 1Mbps.
- **max_bitrates_upload**
  When this entry is set at 1 or more, the value of the [Upload bandwidth] security policy is forcibly changed to this entry value and upload speed is restricted for all VPN sessions connected to the Virtual Hub. For instance, setting this value at 1000000 means that all VPN connection sessions on this Virtual Hub are not able to exceed the upload speed of 1Mbps.
- **max_multilogins_per_user**
  When this entry is set at 1 or more, the multiple login limit security policy for all users connected to the Virtual Hub is permanently overwritten with this value (although when the multiple login limit is set and is smaller than the value designated in here then that multiple login limit value is used).
- **deny_empty_password**
  When this entry is 1 (Enabled), users registered on the Virtual Hub are unable to set empty passwords. If there are users who have set empty passwords, they are unable to connect to the VPN (except connections from localhost, which are possible).
- **deny_bridge**
  When this entry is 1 (Enabled), bridge is permanently denied for sessions connected to the Virtual Hub regardless of the contents of the user's security policies when connected. It is therefore not possible to connect to the Virtual Hub with the aim of bridging.
- **deny_qos**
  When this entry is 1 (Enabled), the VoIP / QoS support function is permanently disabled for sessions connected to the Virtual Hub regardless of the contents of the user's security policies when connected.
- **deny_routing**
  When this entry is 1 (Enabled), routing is permanently denied for sessions connected to the Virtual Hub regardless of the contents of the user's security

policies when connected. It is therefore not possible to connect to the Virtual Hub with the aim of routing.

- **deny_change_user_password**
  When this entry is 1 (Enabled), Virtual Hub users are unable to change their own passwords in the password authentication mode.
- **no_change_users**
  When this entry is 1 (Enabled), Virtual Hub Administrators are unable to add new users or delete or edit existing users on the Virtual Hub.
- **no_change_groups**
  When this entry is 1 (Enabled), Virtual Hub Administrators are unable to add new groups or delete or edit existing groups on the Virtual Hub.
- **no_SecureNAT**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot enable or disable the SecureNAT function.
- **no_SecureNAT_enabledhcp**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot enable the Virtual DHCP Server in the SecureNAT function.
- **no_SecureNAT_enablenat**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot enable virtual NAT function in the SecureNAT function.
- **no_cascade**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot create, delete or edit cascade connections or put them online/ take them offline.
- **no_online**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot put an offline Virtual Hub online.
- **no_offline**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot take an online Virtual Hub offline.
- **no_change_log_config**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot modify the save settings of the Virtual Hub log files.
- **no_disconnect_session**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot forcefully disconnect designated VPN sessions connected to the Virtual Hub.
- **no_delete_iptable**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot delete designated IP address entries from the Virtual Hub's IP Address Table database.
- **no_delete_mactable**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot delete designated MAC address entries from the Virtual Hub's MAC Address Table database.
- **no_enum_session**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot enumerate a list of VPN sessions currently connected to the Virtual Hub.

- **no_query_session**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot obtain detailed information on a designated VPN session currently connected to the Virtual Hub.
- **no_change_admin_password**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot change the Virtual Hub administration password.
- **no_change_log_switch_type**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot modify the settings of the [Log file switch cycle] in the Virtual Hub log file save settings.
- **no_change_access_list**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot operate the Virtual Hub's access list.
- **no_change_access_control_list**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot operate the Virtual Hub's IP access control list.
- **no_change_cert_list**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot operate the trusted CA certificates list.
- **no_change_crl_list**
  When this entry is 1 (Enabled), Virtual Hub Administrators cannot operate the Certificates Revocation List.
- **no_read_log_file**
  When this entry is 1 (Enabled), Virtual Hub Administrators are unable to enumerate the Virtual Hub's log file or to remotely read it using an administration connection.

See Also

- 2.2 User Authentication
- 3.4 Virtual Hub Functions
- 4.5 Connect to VPN Server
- 6.3.63 "HubList": Get List of Virtual Hubs
- 6.4.6 "SetEnumDeny": Deny Enumeration by Virtual Hub Anonymous Users
- 6.4.8 "RadiusServerSet": Set RADIUS Server to use for User Authentication
- 6.4.58 "UserList": Get List of Users
- 6.4.59 "UserCreate": Create User
- 6.4.60 "UserSet": Change User Information
- 6.4.61 "UserDelete": Delete User
- 6.4.62 "UserGet": Get User Information