6.4 VPN Server / VPN Bridge Management Command Reference (For Virtual Hub)

This section describes the commands for configuring and managing a Virtual Hub selected with the **Hub** command from among the commands that can be called when using vpncmd in VPN Server or VPN Bridge management mode. For information about the commands for configuring and managing the entire VPN Server, please refer to 6.3 VPN Server / VPN Bridge Management Command Reference (For Entire Server).

6.4.1 "Online": Switch Virtual Hub to Online

Command Name	**Online**
Purpose	Switch Virtual Hub to Online
Description	Use this when the Virtual Hub currently being managed is offline to switch it to online. A Virtual Hub with an offline status cannot receive VPN connections from clients. By switching the Virtual Hub to online, that Virtual Hub becomes able to receive connections from users and provide services. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*Online*
Arguments for "Online":	
No arguments are required.	

6.4.2 "Offline": Switch Virtual Hub to Offline

Command Name	**Offline**
Purpose	Switch Virtual Hub to Offline
Description	Use this when the Virtual Hub currently being managed is online to switch it to offline. If there are sessions currently connected to the Virtual Hub, all sessions will be disconnected. A Virtual Hub with an offline status cannot receive VPN connections from clients. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*Offline*

Arguments for "Offline":
No arguments are required.

6.4.3 "SetMaxSession": Set the Max Number of Concurrently Connected Sessions for Virtual Hub

Command Name	SetMaxSession
Purpose	Set the Max Number of Concurrently Connected Sessions for Virtual Hub
Description	Use this to set the maximum number of sessions that can be concurrently connected to the Virtual Hub that is currently being managed. When there are more sessions than the maximum number of concurrently connected sessions that are being connected from the VPN Client or VPN Bridge, when the maximum number of sessions is reached, clients will no longer be able to connect. This limit on the maximum number of concurrently connected sessions does not include sessions generated in the Virtual Hub by Local Bridges, Virtual NAT, and Cascade Connections. You can get the current setting for the max number of concurrently connected sessions by using the OptionsGet command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SetMaxSession [max_session]*
Arguments for "SetMaxSession":	
max_session	Using an integer, specify the maximum number of concurrently connected sessions to set. Specifying 0 results in a setting of unlimited.

6.4.4 "SetHubPassword": Set Virtual Hub Administrator Password

Command Name	SetHubPassword
Purpose	Set Virtual Hub Administrator Password
Description	Use this to set the Administrator Password for the Virtual Hub that is currently being managed. When a Virtual Hub administrator password has been set, you are able to connect to that Virtual Hub from a VPN Server connection utility in Virtual Hub Admin Mode, by specifying the password. It is also possible to make a VPN connection from a VPN client or VPN Bridge by specifying

	"Administrator" for the user name and the password for the Virtual Hub administrator password. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SetHubPassword [password]*
Arguments for "SetHubPassword":	
password	Specify the password you wish to set. If a password is not specified by parameter, a prompt will appear to input the password.

6.4.5 "SetEnumAllow": Allow Enumeration by Virtual Hub Anonymous Users

Command Name	**SetEnumAllow**
Purpose	Allow Enumeration by Virtual Hub Anonymous Users
Description	Use this to change the options setting of the Virtual Hub you are currently managing to allow anonymous users to enumerate this Virtual Hub. By setting this option, it makes it possible for VPN Client users to enumerate this Virtual Hub simply by inputting this VPN Server address. Also, by using the SetEnumDeny command, you can deny anonymous users the ability to enumerate. At the time a Virtual Hub is created, enumeration will be allowed. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SetEnumAllow*
Arguments for "SetEnumAllow":	
No arguments are required.	

6.4.6 "SetEnumDeny": Deny Enumeration by Virtual Hub Anonymous Users

Command Name	**SetEnumDeny**
Purpose	Deny Enumeration by Virtual Hub Anonymous Users
Description	Use this to change the options setting of the Virtual Hub you are currently managing to prevent anonymous users from enumerating this Virtual Hub. By setting this option, the VPN Client user will be unable to enumerate this Virtual Hub even if they send a Virtual Hub

	enumeration request to the VPN Server. Also, by using the SetEnumAllow command, you can allow anonymous users to enumerate. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SetEnumDeny*
Arguments for "SetEnumDeny":	
No arguments are required.	

6.4.7 "OptionsGet": Get Options Setting of Virtual Hubs

Command Name	**OptionsGet**
Purpose	Get Options Setting of Virtual Hubs
Description	Use this to get a list of the Options setting of the Virtual Hub currently being managed. You can get the following: Allow/Deny Virtual Hub Enumeration, Maximum Concurrent Connections, Online/Offline Status, and Virtual Hub Type in Clustering Environment. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*OptionsGet*
Arguments for "OptionsGet":	
No arguments are required.	

6.4.8 "RadiusServerSet": Set RADIUS Server to use for User Authentication

Command Name	**RadiusServerSet**
Purpose	Set RADIUS Server to use for User Authentication
Description	To accept users to the currently managed Virtual Hub in RADIUS server authentication mode, you can specify an external RADIUS server that confirms the user name and password. (You can specify multiple hostname by splitting with comma or semicolon.) The RADIUS server must be set to receive requests from IP addresses of this VPN Server. Also, authentication by Password Authentication Protocol (PAP) must be enabled. This command cannot be run on VPN Bridge.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*RadiusServerSet [server_name:port] [/SECRET:secret] [/RETRY_INTERVAL:interval]*
Arguments for "RadiusServerSet":	
server_name:port	Using the format "host name:port number", specify the host name or IP address, and the UDP port number of the RADIUS server being used. If the port number is omitted, 1812 will be used. You can specify multiple hostname by splitting with comma or semicolon.
/SECRET	Specify the shared secret (password) used for communication with the RADIUS Server

6.4.9 "RadiusServerDelete": Delete Setting to Use RADIUS Server for User Authentication

Command Name	**RadiusServerDelete**
Purpose	Delete Setting to Use RADIUS Server for User Authentication
Description	Use this to delete the setting related to using a RADIUS server when a user connects to the currently managed Virtual Hub in RADIUS Server Authentication Mode and disable the RADIUS authentication. To get the settings related to the current RADIUS server use the RadiusServerGet command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*RadiusServerDelete*
Arguments for "RadiusServerDelete":	
No arguments are required.	

6.4.10 "RadiusServerGet": Get Setting of RADIUS Server Used for User Authentication

Command Name	**RadiusServerGet**
Purpose	Get Setting of RADIUS Server Used for User Authentication
Description	Use this to get the current settings for the RADIUS server used when a user connects to the currently managed Virtual Hub using RADIUS Server Authentication Mode. This command cannot be run on VPN Bridge.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*RadiusServerGet*
Arguments for "RadiusServerGet":	
No arguments are required.	

6.4.11 "StatusGet": Get Current Status of Virtual Hub

Command Name	**StatusGet**
Purpose	Get Current Status of Virtual Hub
Description	Use this to get the current status of the Virtual Hub currently being managed. You can get the following information: Virtual Hub Type, Number of Sessions, Number of Each Type of Object, Number of Logins, Last Login, Last Communication, and Communication Statistical Data.
Command-line	*StatusGet*
Arguments for "StatusGet":	
No arguments are required.	

6.4.12 "LogGet": Get Log Save Setting of Virtual Hub

Command Name	**LogGet**
Purpose	Get Log Save Setting of Virtual Hub
Description	Use this to get the log save setting for the Virtual Hub that is currently being managed. You can get the setting information such as the save setting related to security logs and packet logs and information on what is saved.
Command-line	*LogGet*
Arguments for "LogGet":	
No arguments are required.	

6.4.13 "LogEnable": Enable Security Log or Packet Log

Command Name	**LogEnable**
Purpose	Enable Security Log or Packet Log

Description	Use this to enable a security log or packet log of the Virtual Hub currently being managed. To get the current setting, you can use the LogGet command.
Command-line	*LogEnable [security|packet]*
Arguments for "LogEnable":	
security|packet	Select the type of log to enable. Specify either "security" or "packet".

6.4.14 "LogDisable": Disable Security Log or Packet Log

Command Name	**LogDisable**
Purpose	Disable Security Log or Packet Log
Description	Use this to disable a security log or packet log of the Virtual Hub currently being managed. To get the current setting, you can use the LogGet command.
Command-line	*LogDisable [security|packet]*
Arguments for "LogDisable":	
security|packet	Select the type of log to disable. Specify either "security" or "packet".

6.4.15 "LogSwitchSet": Set Log File Switch Cycle

Command Name	**LogSwitchSet**
Purpose	Set Log File Switch Cycle
Description	Use this to set the log file switch cycle for the security log or packet log that the currently managed Virtual Hub saves. The log file switch cycle can be changed to switch in every second, every minute, every hour, every day, every month ,or not switch. To get the current setting, you can use the LogGet command.
Command-line	*LogSwitchSet [security|packet]* *[/SWITCH:sec|min|hour|day|month|none]*
Arguments for "LogSwitchSet":	
security|packet	Select the type of log to change setting. Specify either "security" or "packet".
/SWITCH	Select the switch cycle to set. Specify sec, min, hour, day, month or none.

6.4.16 "LogPacketSaveType": Set Save Contents and Type of Packet to Save to Packet Log

Command Name	**LogPacketSaveType**
Purpose	Set Save Contents and Type of Packet to Save to Packet Log
Description	Use this to set the save contents of the packet log for each type of packet to be saved by the currently managed Virtual Hub. There are the following packet types: TCP Connection Log, TCP Packet Log, DHCP Packet Log, UDP Packet Log, ICMP Packet Log, IP Packet Log, ARP Packet Log, and Ethernet Packet Log. To get the current setting, you can use the LogGet command.
Command-line	*LogPacketSaveType* *[/TYPE:tcpconn|tcpdata|dhcp|udp|icmp|ip|arp|ether]* *[/SAVE:none|header|full]*
Arguments for "LogPacketSaveType":	
/TYPE	Specify tcpconn, tcpdata, dhcp, udp, icmp, ip, arp, or ether to specify the type of packet whose save contents are going to be changed.
/SAVE	Specify the save contents of the packet log. Specify either none: save nothing header: header information only full: all packet contents

6.4.17 "CAList": Get List of Trusted CA Certificates

Command Name	**CAList**
Purpose	Get List of Trusted CA Certificates
Description	Here you can manage the certificate authority certificates that are trusted by this currently managed Virtual Hub. The list of certificate authority certificates that are registered is used to verify certificates when a VPN Client is connected in signed certificate authentication mode. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*CAList*
Arguments for "CAList":	
No arguments are required.	

6.4.18 "CAAdd": Add Trusted CA Certificate

Command Name	**CAAdd**
Purpose	Add Trusted CA Certificate
Description	Use this to add a new certificate to a list of CA certificates trusted by the currently managed Virtual Hub. The list of certificate authority certificates that are registered is used to verify certificates when a VPN Client is connected in signed certificate authentication mode. To get a list of the current certificates you can use the CAList command. The certificate you add must be saved in the X.509 file format. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*CAAdd [path]*
Arguments for "CAAdd":	
path	Specify the file name of the X.509 certificate to register.

6.4.19 "CADelete": Delete Trusted CA Certificate

Command Name	**CADelete**
Purpose	Delete Trusted CA Certificate
Description	Use this to delete an existing certificate from the list of CA certificates trusted by the currently managed Virtual Hub. To get a list of the current certificates you can use the CAList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*CADelete [id]*
Arguments for "CADelete":	
id	Specify the ID of the certificate to delete.

6.4.20 "CAGet": Get Trusted CA Certificate

Command Name	**CAGet**
Purpose	Get Trusted CA Certificate

Description	Use this to get an existing certificate from the list of CA certificates trusted by the currently managed Virtual Hub and save it as a file in X.509 format. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*CAGet [id] [/SAVECERT:path]*
Arguments for "CAGet":	
id	Specify the ID of the certificate to get.
/SAVECERT	Specify the file name to save the certificate you obtained.

6.4.21 "CascadeList": Get List of Cascade Connections

Command Name	**CascadeList**
Purpose	Get List of Cascade Connections
Description	Use this to get a list of Cascade Connections that are registered on the currently managed Virtual Hub. By using a Cascade Connection, you can connect this Virtual Hub by Layer 2 Cascade Connection to another Virtual Hub that is operating on the same or a different computer. [Warning About Cascade Connections] By connecting using a Cascade Connection you can create a Layer 2 bridge between multiple Virtual Hubs but if the connection is incorrectly configured, a loopback Cascade Connection could inadvertently be created. When using a Cascade Connection function please design the network topology with care. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeList*
Arguments for "CascadeList":	
No arguments are required.	

6.4.22 "CascadeCreate": Create New Cascade Connection

Command Name	**CascadeCreate**
Purpose	Create New Cascade Connection
Description	Use this to create a new Cascade Connection on the currently managed Virtual Hub.

	By using a Cascade Connection, you can connect this Virtual Hub by Cascade Connection to another Virtual Hub that is operating on the same or a different computer. To create a Cascade Connection, you must specify the name of the Cascade Connection, destination server and destination Virtual Hub and user name. When a new Cascade Connection is created, the type of user authentication is initially set as Anonymous Authentication and the proxy server setting and the verification options of the server certificate is not set. To change these settings and other advanced settings after a Cascade Connection has been created, use the other commands that begin with the name "Cascade". [Warning About Cascade Connections] By connecting using a Cascade Connection you can create a Layer 2 bridge between multiple Virtual Hubs but if the connection is incorrectly configured, a loopback Cascade Connection could inadvertently be created. When using a Cascade Connection function please design the network topology with care. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeCreate [name] [/SERVER:hostname:port] [/HUB:hubname] [/USERNAME:username]*
Arguments for "CascadeCreate":	
name	Specify the name of the Cascade Connection to create.
/SERVER	Specify the host name and port number of the destination VPN Server using the format [host name:port number]. You can also specify by IP address.
/HUB	Specify the Virtual Hub on the destination VPN Server.
/USERNAME	Specify the user name to use for user authentication when connecting to the destination VPN Server.

6.4.23 "CascadeSet": Set the Destination for Cascade Connection

Command Name	**CascadeSet**
Purpose	Set the Destination for Cascade Connection
Description	Use this to set the destination VPN Server host name and port number, Virtual Hub name and the user name that will use the connection for the Cascade Connection registered on the currently managed virtual Hub.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeSet [name] [/SERVER:hostname:port] [/HUB:hubname]*
Arguments for "CascadeSet":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/SERVER	Specify the host name and port number of the destination VPN Server using the format [host name:port number]. You can also specify by IP address.
/HUB	Specify the Virtual Hub on the destination VPN Server.

6.4.24 "CascadeGet": Get the Cascade Connection Setting

Command Name	**CascadeGet**
Purpose	Get the Cascade Connection Setting
Description	Use this to get the Connection Setting of a Cascade Connection that is registered on the currently managed Virtual Hub. To change the Connection Setting contents of the Cascade Connection, use the other commands that begin with the name "Cascade" after creating the Cascade Connection. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeGet [name]*
Arguments for "CascadeGet":	
name	Specify the name of the Cascade Connection whose setting you want to get.

6.4.25 "CascadeDelete": Delete Cascade Connection Setting

Command Name	**CascadeDelete**
Purpose	Delete Cascade Connection Setting
Description	Use this to delete a Cascade Connection that is registered on the currently managed Virtual Hub. If the specified Cascade Connection has a status of online, the connections will be automatically disconnected and then the Cascade Connection will be deleted. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeDelete [name]*

Arguments for "CascadeDelete":	
name	Specify the name of the Cascade Connection to delete.

6.4.26 "CascadeUsernameSet": Set User Name to Use Connection of Cascade Connection

Command Name	CascadeUsernameSet
Purpose	Set User Name to Use Connection of Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to the VPN Server, use this to specify the user name required for user authentication. In some cases it is necessary to specify the type of user authentication and specify the required parameters. To change this information you can use commands such as CascadeAnonymousSet, CascadePasswordSet, and CascadeCertSet. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeUsernameSet [name] [/USERNAME:username]*
Arguments for "CascadeUsernameSet":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/USERNAME	Specify the user name required for user authentication when the Cascade Connection connects to the VPN Server.

6.4.27 "CascadeAnonymousSet": Set User Authentication Type of Cascade Connection to Anonymous Authentication

Command Name	CascadeAnonymousSet
Purpose	Set User Authentication Type of Cascade Connection to Anonymous Authentication
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to the VPN Server, set the user authe type to [anonymous authentication]. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeAnonymousSet [name]*
Arguments for "CascadeAnonymousSet":	

name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.28 "CascadePasswordSet": Set User Authentication Type of Cascade Connection to Password Authentication

Command Name	**CascadePasswordSet**
Purpose	Set User Authentication Type of Cascade Connection to Password Authentication
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to the VPN Server, use this to set the user auth type to Password Authentication. Specify Standard Password Authentication and RADIUS or NT Domain Authentication as the password authentication type. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadePasswordSet [name] [/PASSWORD:password] [/TYPE:standard|radius]*
Arguments for "CascadePasswordSet":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/PASSWORD	Specify the password to use for password authentication. If this is not specified, a prompt will appear to input the password.
/TYPE	Specify either "standard" (Standard Password Authentication) or "radius" (RADIUS or NT Domain Authentication) as the password authentication type.

6.4.29 "CascadeCertSet": Set User Authentication Type of Cascade Connection to Client Certificate Authentication

Command Name	**CascadeCertSet**
Purpose	Set User Authentication Type of Cascade Connection to Client Certificate Authentication
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to the VPN Server, use this to set the user auth type to Client Certificate Authentication. For this certificate, you must specify a certificate file in the X.509 format and a private key file that is Base 64 encoded.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeCertSet [name] [/LOADCERT:cert] [/LOADKEY:key]*
Arguments for "CascadeCertSet":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/LOADCERT	Specify the X.509 format certificate file to provide for certificate authentication.
/LOADKEY	Specify the Base-64-encoded private key file name for the certificate.

6.4.30 "CascadeCertGet": Get Client Certificate to Use for Cascade Connection

Command Name	**CascadeCertGet**
Purpose	Get Client Certificate to Use for Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection uses client certificate authentication, use this to get the certificate that is provided as the client certificate and save the certificate file in X.509 format. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeCertGet [name] [/SAVECERT:cert]*
Arguments for "CascadeCertGet":	
name	Specify the name of the Cascade Connection whose setting you want to get.
/SAVECERT	Specify the file name to save the certificate you obtained in X.509 format.

6.4.31 "CascadeEncryptEnable": Enable Encryption when Communicating by Cascade Connection

Command Name	**CascadeEncryptEnable**
Purpose	Enable Encryption when Communicating by Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection is used for communication between VPN Servers via a VPN connection, use this to set the communication contents between the VPN Servers to be

	encrypted by SSL. Normally communication between VPN Servers is encrypted by SSL to prevent eavesdropping of information and fraud. You can also disable encryption. When encryption is disabled, the communication throughput improves but the communication data flows over the network in plain text. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeEncryptEnable [name]*
Arguments for "CascadeEncryptEnable":	
name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.32 "CascadeEncryptDisable": Disable Encryption when Communicating by Cascade Connection

Command Name	**CascadeEncryptDisable**
Purpose	Disable Encryption when Communicating by Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection is used for communication between VPN Servers via a VPN connection, use this to set the communication contents between the VPN Servers not to be encrypted. Normally communication between VPN Servers is encrypted by SSL to prevent eavesdropping of information and fraud. You can also disable encryption. When encryption is disabled, the communication throughput improves but the communication data flows over the network in plain text. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeEncryptDisable [name]*
Arguments for "CascadeEncryptDisable":	
name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.33 "CascadeCompressEnable": Enable Data Compression when Communicating by Cascade Connection

Command Name	**CascadeCompressEnable**

Purpose	Enable Data Compression when Communicating by Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection is used for communication between VPN Servers via a VPN connection, use this to set the communication contents between the VPN Servers to be compressed. It is possible to achieve a maximum of 80% compression. Compression however places higher loads on the CPU of both the client and server machines. When the line speed is about 10 Mbps or greater, compression can lower throughput, but sometimes it can have the opposite effect. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeCompressEnable [name]*
Arguments for "CascadeCompressEnable":	
name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.34 "CascadeCompressDisable": Disable Data Compression when Communicating by Cascade Connection

Command Name	**CascadeCompressDisable**
Purpose	Disable Data Compression when Communicating by Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection is used for communication between VPN Servers via a VPN connection, use this to set the communication contents between the VPN Servers to be not compressed. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeCompressDisable [name]*
Arguments for "CascadeCompressDisable":	
name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.35 "CascadeProxyNone": Specify Direct TCP/IP Connection as the Connection Method of Cascade Connection

Command Name	**CascadeProxyNone**
Purpose	Specify Direct TCP/IP Connection as the Connection Method of Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to a VPN Server, use this to set Direct TCP/IP Connection as the connection method to use, in which case the connection route will not be via a proxy server. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeProxyNone [name]*
Arguments for "CascadeProxyNone":	
name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.36 "CascadeProxyHttp": Set Connection Method of Cascade Connection to be via an HTTP Proxy Server

Command Name	**CascadeProxyHttp**
Purpose	Set Connection Method of Cascade Connection to be via an HTTP Proxy Server
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to a VPN Server, use this to set Connect via HTTP Proxy Server as the method of connection to use, which requires the specification of the host name and port number of the HTTP Proxy server to communicate via as well as a user name and password (when required). The HTTP server that communication will travel via must be compatible with the CONNECT method to use HTTPS communication. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeProxyHttp [name] [/SERVER:hostname:port] [/USERNAME:username] [/PASSWORD:password]*
Arguments for "CascadeProxyHttp":	
name	Specify the name of the Cascade Connection whose setting you want to change.

/SERVER	Specify the host name or IP address, and port number of the on-route HTTP proxy server using the format [host name:port number].
/USERNAME	When user authentication is required to connect to the on-route HTTP proxy server, specify the user name. Also, specify the /PASSWORD parameter at the same time. If the parameters /USERNAME and /PASSWORD are not specified, the user authentication data will not be set.
/PASSWORD	When user authentication is required to connect to the on-route HTTP proxy server, specify the password. Specify this together with the /USERNAME parameter.

6.4.37 "CascadeProxySocks": Set Connection Method of Cascade Connection to be via an SOCKS Proxy Server

Command Name	**CascadeProxySocks**
Purpose	Set Connection Method of Cascade Connection to be via an SOCKS Proxy Server
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to a VPN Server, use this to set Connect via SOCKS Proxy Server as the method of connection to use, which requires the specification of the host name and port number of the SOCKS Proxy server to communicate via as well as a user name and password (when required). The on-route SOCKS server must be compatible with SOCKS Version 4. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeProxySocks [name] [/SERVER:hostname:port] [/USERNAME:username] [/PASSWORD:password]*
Arguments for "CascadeProxySocks":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/SERVER	Specify the host name or IP address, and port number of the on-route SOCKS proxy server using the format "host name:port number".
/USERNAME	When user authentication is required to connect to the on-route SOCKS proxy server, specify the user name. Also, specify the /PASSWORD parameter at the same time. If the parameters /USERNAME and /PASSWORD are not specified, the user authentication data will not be set.

/PASSWORD	When user authentication is required to connect to the on-route SOCKS proxy server, specify the password. Specify this together with the /USERNAME parameter.

6.4.38 "CascadeServerCertEnable": Enable Cascade Connection Server Certificate Verification Option

Command Name	**CascadeServerCertEnable**
Purpose	Enable Cascade Connection Server Certificate Verification Option
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to a VPN Server, use this to enable the option to check whether the SSL certificate provided by the destination VPN Server can be trusted. If this option is enabled you must either use the CascadeServerCertSet command to save the connection destination server SSL certificate beforehand in the Cascade Connection Settings beforehand, or use the CAAdd command etc. to register a root certificate containing the signed server SSL certificate in the list of Virtual Hub trusted CA certificates. If the certificate of the connected VPN Server cannot be trusted under the condition where the option to verify server certificates was enabled for the Cascade Connection, the connection will be promptly cancelled and continual reattempts at connection will be made. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeServerCertEnable [name]*
Arguments for "CascadeServerCertEnable":	
name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.39 "CascadeServerCertDisable": Disable Cascade Connection Server Certificate Verification Option

Command Name	**CascadeServerCertDisable**
Purpose	Disable Cascade Connection Server Certificate Verification Option
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to a VPN Server, use this to disable the option to check whether the SSL certificate provided by the destination VPN Server can be trusted.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeServerCertDisable [name]*
Arguments for "CascadeServerCertDisable":	
name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.40 "CascadeServerCertSet": Set the Server Individual Certificate for Cascade Connection

Command Name	**CascadeServerCertSet**
Purpose	Set the Server Individual Certificate for Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to a VPN Server, use this to register beforehand the same certificate as the SSL certificate provided by the destination VPN Server. If the option to verify server certificates for Cascade Connections is enabled, you must either use this command to save the connection destination server SSL certificate beforehand in the Cascade Connection Settings beforehand, or use the CAAdd command etc. to register a root certificate containing the signed server SSL certificate in the list of Virtual Hub trusted CA certificates. If the certificate of the connected VPN Server cannot be trusted under the condition where the option to verify server certificates was enabled for the Cascade Connection, the connection will be promptly cancelled and continual reattempts at connection will be made. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeServerCertSet [name] [/LOADCERT:cert]*
Arguments for "CascadeServerCertSet":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/LOADCERT	Specify X.509 format certificate file name that the server individual certificate you wish to set is saved under.

6.4.41 "CascadeServerCertDelete": Delete the Server Individual Certificate for Cascade Connection

Command Name	**CascadeServerCertDelete**

Purpose	Delete the Server Individual Certificate for Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and a server individual certificate is registered for that Cascade Connection, use this to delete that server individual certificate. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeServerCertDelete [name]*
Arguments for "CascadeServerCertDelete":	
name	Specify the name of the Cascade Connection whose setting you want to change.

6.4.42 "CascadeServerCertGet": Get the Server Individual Certificate for Cascade Connection

Command Name	**CascadeServerCertGet**
Purpose	Get the Server Individual Certificate for Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and a server individual certificate is registered for that Cascade Connection, use this to get that certificate and save it as an X.509 format certificate file. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeServerCertGet [name] [/SAVECERT:path]*
Arguments for "CascadeServerCertGet":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/SAVECERT	Specify the certificate file name to save the server individual certificate in X.509 format.

6.4.43 "CascadeDetailSet": Set Advanced Settings for Cascade Connection

Command Name	**CascadeDetailSet**
Purpose	Set Advanced Settings for Cascade Connection
Description	Use this to customize the VPN protocol communication settings used when a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection connects to the

	VPN Server. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeDetailSet [name] [/MAXTCP:max_connection] [/INTERVAL:interval] [/TTL:disconnect_span] [/HALF:yes|no] [/NOQOS:yes|no]*
Arguments for "CascadeDetailSet":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/MAXTCP	Specify, using an integer in the range 1 to 32, the number of TCP connections to be used for VPN communication. By using data transmission by multiple TCP connections for VPN communication sessions with VPN Servers it is sometimes possible to increase communication speed. Note: We recommend about 8 lines when the connection lines to the server are fast, and 1 line when using a slow connection such as dialup.
/INTERVAL	When communicating by VPN by establishing multiple TCP connections, specify in seconds, the establishing interval for each TCP connection. The standard value is 1 second.
/TTL	When specifying connection life of each TCP connection specify in seconds the keep-alive time from establishing a TCP connection until disconnection. If 0 is specified, keep-alive will not be set.
/HALF	Specify "yes" when enabling half duplex mode. When using two or more TCP connections for VPN communication, it is possible to use Half Duplex Mode. By enabling half duplex mode it is possible to automatically fix data transmission direction as half and half for each TCP connection. In the case where a VPN using 8 TCP connections is established, for example, when half-duplex is enabled, communication can be fixes so that 4 TCP connections are dedicated to the upload direction and the other 4 connections are dedicated to the download direction.
/NOQOS	Specify "yes" when disabling VoIP / QoS functions. Normally "no" is specified.

6.4.44 "CascadePolicySet": Set Cascade Connection Session Security Policy

Command Name	**CascadePolicySet**
Purpose	Set Cascade Connection Session Security Policy
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection is established,

	use this to change the security policy contents that are applied to the session generated by the Virtual Hub. When a Virtual Hub makes a Cascade Connection to another VPN Server, a Cascade Session will be newly generated on the Virtual Hub that is the Cascade Connection source. You can use this command to set the security policy contents that will set this Cascade session. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*[name] [/NAME:policy_name] [/VALUE:num|yes|no]*
Arguments for "CascadePolicySet":	
name	Specify the name of the Cascade Connection whose setting you want to change.
/NAME	Specify the name of policy whose values you want to change. You can use the PolicyList command to display a list of policy names and values that can be set.
/VALUE	Specify a new policy value. If the policy is an integer value, specify an integer. Specify yes or no for Boolean types. You can view the type and value that can be set by using the PolicyList command.

6.4.45 "PolicyList": Display List of Security Policy Types and Settable Values

Command Name	**PolicyList**
Purpose	Display List of Security Policy Types and Settable Values
Description	Use this to display a list of item names, descriptions, and settable values in the security policies that can be set for VPN Server users and groups and Cascade Connections. By running the PolicyList command without specifying any parameters, a list of all supported security policy names and descriptions will be displayed. By specifying the name using the PolicyList command parameter, a detailed description related to this value and the type and range of the settable value will be displayed.
Command-line	*PolicyList [name]*
Arguments for "PolicyList":	
name	This allows you to specify the policy name whose description you want to display. If you don't specify a name, a list of all supported security names and descriptions will be displayed.

6.4.46 "CascadeStatusGet": Get Current Cascade Connection Status

Command Name	**CascadeStatusGet**
Purpose	Get Current Cascade Connection Status
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified and that Cascade Connection is currently online, use this to get its connection status and other information. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeStatusGet [name]*
Arguments for "CascadeStatusGet":	
name	Specify the name of the Cascade Connection whose information you want to get.

6.4.47 "CascadeRename": Change Name of Cascade Connection

Command Name	**CascadeRename**
Purpose	Change Name of Cascade Connection
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified, use this to change the name of that Cascade Connection. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeRename [name] [/NEW:new_name]*
Arguments for "CascadeRename":	
name	Specify the current name of the Cascade Connection whose name you want to change.
/NEW	Specify the new name after the change.

6.4.48 "CascadeOnline": Switch Cascade Connection to Online Status

Command Name	**CascadeOnline**
Purpose	Switch Cascade Connection to Online Status
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified, use this to switch that Cascade Connection to online status. The Cascade Connection that is switched to online status begins the process of connecting to the destination VPN Server in accordance with the Connection Setting. The Cascade Connection

	that is switched to online status will establish normal connection to the VPN Server or continue to attempt connection until it is switched to offline status. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeOnline [name]*
Arguments for "CascadeOnline":	
name	Specify the name of the Cascade Connection to switch to online status.

6.4.49 "CascadeOffline": Switch Cascade Connection to Offline Status

Command Name	**CascadeOffline**
Purpose	Switch Cascade Connection to Offline Status
Description	When a Cascade Connection registered on the currently managed Virtual Hub is specified, use this to switch that Cascade Connection to offline status. The Cascade Connection that is switched to offline will not connect to the VPN Server until next time it is switched to the online status using the CascadeOnline command You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CascadeOffline [name]*
Arguments for "CascadeOffline":	
name	Specify the name of the Cascade Connection to switch to offline status.

6.4.50 "AccessAdd": Add Access List Rules (IPv4)

Command Name	**AccessAdd**
Purpose	Add Access List Rules (IPv4)
Description	Use this to add a new rule to the access list of the currently managed Virtual Hub. The access list is a set of packet file rules that are applied to packets that flow through the Virtual Hub. You can register multiple rules in an access list and you can also define an priority for each rule. All packets are checked for the conditions specified by the rules registered in the access list and based on the operation that is stipulated by the first matching rule, they either pass or are discarded. Packets that do not match any rule are implicitly allowed

	to pass. You can also use the AccessAddEx command to generate delays, jitters and packet losses. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*AccessAdd [pass|discard] [/MEMO:memo] [/PRIORITY:priority] [/SRCUSERNAME:username] [/DESTUSERNAME:username] [/SRCMAC:mac/mask] [/DESTMAC:mac/mask] [/SRCIP:ip/mask] [/DESTIP:ip/mask] [/PROTOCOL:tcp|udp|icmpv4|icmpv6|ip|num] [/SRCPORT:start-end] [/DESTPORT:start-end] [/TCPSTATE: established|unestablished]*
Arguments for "AccessAdd":	
pass|discard	When a packet matches this rule condition, this operation is decided. When pass is specified, the packet is allowed to pass, and when discard is specified, the packet is discarded.
/MEMO	Specify a description (memo) for this rule.
/PRIORITY	Specify an integer of 1 or higher to indicate the priority of the rule. Higher priority is given to rules with the lower priority values.
/SRCUSERNAME	You can apply this rule to only the packets sent by a user session of a user name that has been specified as a rule condition. In this case, specify the user name.
/DESTUSERNAME	You can apply this rule to only the packets received by a user session of a user name that has been specified as a rule condition. In this case, specify the user name.
/SRCMAC	Specify destination MAC address as a rule. Specify MAC address with "-" or ":" separators and hexadecimal number like "00-AC-84-EA-33-BC/FF-FF-FF-FF-FF-00". The separators are skippable.
/DESTMAC	Specify destination MAC address as a rule. Use the same method of specification as for the /SRCMAC parameter.
/SRCIP	Specify a source IPv4 address as a rule condition. Specify the IPv4 address in the format of "IP Address/Mask" by separating the decimal values using dots such as "192.168.0.1". For the mask, either specify decimal values separated by dots such as "255.255.255.0", or you can specify the bit length from the header using a decimal value such as "24". If you specify "0.0.0.0/0.0.0.0", this means all hosts.
/DESTIP	Specify a destination IPv4 address as a rule condition in the format of "IP Address/Mask". Use the same method of specification as for the /SRCIP parameter.
/PROTOCOL	Specify a protocol type as a rule condition. Input the IP protocol number using decimal values or specify one of the keywords "tcp" (TCP/IP protocol, no.6), "udp" (UDP/IP protocol, no.17), "icmpv4" (ICMPv4 protocol, no.1), "icmpv6" (ICMPv6 protocol, no.58) or

	"ip" (all protocols, no.0). Specify 0 to make the rule apply to all IP protocols.
/SRCPORT	If the specified protocol is TCP/IP or UDP/IP, specify the source port number as the rule condition. Protocols other than this will be ignored. When this parameter is not specified, the rules will apply to all port numbers. When specifying, do so using the following method "1-1024" (1 to 1024), "23" (only 23).
/DESTPORT	If the specified protocol is TCP/IP or UDP/IP, specify the destination port number as the rule condition. Protocols other than this will be ignored. Use the same method of specification as for the /SRCPORT parameter.
/TCPSTATE	Specify TCP connection state as a rule. Use Established or Unestablished.

6.4.51 "AccessAddEx": Add Extended Access List Rules (IPv4: Delay, Jitter and Packet Loss Generating)

Command Name	**AccessAddEx**
Purpose	Add Extended Access List Rules (IPv4: Delay, Jitter and Packet Loss Generating)
Description	Use this to add a new rule to the access list of the currently managed Virtual Hub. You can set to generate delays, jitters and packet losses when a packet is passing via the Virtual Hub. The access list is a set of packet file rules that are applied to packets that flow through the Virtual Hub. You can register multiple rules in an access list and you can also define an priority for each rule. All packets are checked for the conditions specified by the rules registered in the access list and based on the operation that is stipulated by the first matching rule, they either pass or are discarded. Packets that do not match any rule are implicitly allowed to pass. You can also use the AccessAddEx command to generate delays, jitters and packet losses. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*AccessAddEx [pass|discard] [/MEMO:memo] [/PRIORITY:priority] [/SRCUSERNAME:username] [/DESTUSERNAME:username] [/SRCMAC:mac/mask] [/DESTMAC:mac/mask] [/SRCIP:ip/mask] [/DESTIP:ip/mask] [/PROTOCOL:tcp|udp|icmpv4|icmpv6|ip|num] [/SRCPORT:start-end] [/DESTPORT:start-end] [/TCPSTATE:*

	established|unestablished] [/DELAY:delay_millisec] [/JITTER:jitter_percent] [/LOSS:loss_percent]
Arguments for "AccessAddEx":	
pass|discard	When a packet matches this rule condition, this operation is decided. When pass is specified, the packet is allowed to pass, and when discard is specified, the packet is discarded. The setting of delays, jitters and packet losses is applied if the action is pass.
/MEMO	Specify a description (memo) for this rule.
/PRIORITY	Specify an integer of 1 or higher to indicate the priority of the rule. Higher priority is given to rules with the lower priority values.
/SRCUSERNAME	You can apply this rule to only the packets sent by a user session of a user name that has been specified as a rule condition. In this case, specify the user name.
/DESTUSERNAME	You can apply this rule to only the packets received by a user session of a user name that has been specified as a rule condition. In this case, specify the user name.
/SRCMAC	Specify destination MAC address as a rule. Specify MAC address with "-" or ":" separators and hexadecimal number like "00-AC-84-EA-33-BC/FF-FF-FF-FF-FF-00". The separators are skippable.
/DESTMAC	Specify destination MAC address as a rule. Use the same method of specification as for the /SRCMAC parameter.
/SRCIP	Specify a source IPv4 address as a rule condition. Specify the IPv4 address in the format of "IP Address/Mask" by separating the decimal values using dots such as "192.168.0.1". For the mask, either specify decimal values separated by dots such as "255.255.255.0", or you can specify the bit length from the header using a decimal value such as "24". If you specify "0.0.0.0/0.0.0.0", this means all hosts.
/DESTIP	Specify a destination IPv4 address as a rule condition in the format of "IP Address/Mask". Use the same method of specification as for the /SRCIP parameter.
/PROTOCOL	Specify a protocol type as a rule condition. Input the IP protocol number using decimal values or specify one of the keywords "tcp" (TCP/IP protocol, no.6), "udp" (UDP/IP protocol, no.17), "icmpv4" (ICMPv4 protocol, no.1), "icmpv6" (ICMPv6 protocol, no.58) or "ip" (all protocols, no.0). Specify 0 to make the rule apply to all IP protocols.
/SRCPORT	If the specified protocol is TCP/IP or UDP/IP, specify the source port number as the rule condition. Protocols other than this will be ignored. When this parameter is not specified, the rules will apply to all port numbers. When specifying, do so using the following method "1-1024" (1 to 1024), "23" (only 23).

/DESTPORT	If the specified protocol is TCP/IP or UDP/IP, specify the destination port number as the rule condition. Protocols other than this will be ignored. Use the same method of specification as for the /SRCPORT parameter.
/TCPSTATE	Specify TCP connection state as a rule. Use Established or Unestablished.
/DELAY	Set this value to generate delays when packets is passing. Specify the delay period in milliseconds. Specify 0 means no delays to generate. The delays must be 10000 milliseconds at most.
/JITTER	Set this value to generate jitters when packets is passing. Specify the ratio of fluctuation of jitters within 0% to 100% range. Specify 0 means no jitters to generate.
/LOSS	Set this value to generate packet losses when packets is passing. Specify the ratio of packet losses within 0% to 100% range. Specify 0 means no packet losses to generate.

6.4.52 "AccessAdd6": Add Access List Rules (IPv6)

Command Name	**AccessAdd6**
Purpose	Add Access List Rules (IPv6)
Description	Use this to add a new rule to the access list of the currently managed Virtual Hub. The access list is a set of packet file rules that are applied to packets that flow through the Virtual Hub. You can register multiple rules in an access list and you can also define an priority for each rule. All packets are checked for the conditions specified by the rules registered in the access list and based on the operation that is stipulated by the first matching rule, they either pass or are discarded. Packets that do not match any rule are implicitly allowed to pass. You can also use the AccessAddEx6 command to generate delays, jitters and packet losses. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*AccessAdd6 [pass|discard] [/MEMO:memo] [/PRIORITY:priority] [/SRCUSERNAME:username] [/DESTUSERNAME:username] [/SRCMAC:mac/mask] [/DESTMAC:mac/mask] [/SRCIP:ip/mask] [/DESTIP:ip/mask] [/PROTOCOL:tcp|udp|icmpv4|icmpv6|ip|num] [/SRCPORT:start-end] [/DESTPORT:start-end] [/TCPSTATE: established|unestablished]*
Arguments for "AccessAdd6":	

pass|discard	When a packet matches this rule condition, this operation is decided. When pass is specified, the packet is allowed to pass, and when discard is specified, the packet is discarded.
/MEMO	Specify a description (memo) for this rule.
/PRIORITY	Specify an integer of 1 or higher to indicate the priority of the rule. Higher priority is given to rules with the lower priority values.
/SRCUSERNAME	You can apply this rule to only the packets sent by a user session of a user name that has been specified as a rule condition. In this case, specify the user name.
/DESTUSERNAME	You can apply this rule to only the packets received by a user session of a user name that has been specified as a rule condition. In this case, specify the user name.
/SRCMAC	Specify destination MAC address as a rule. Specify MAC address with "-" or ":" separators and hexadecimal number like "00-AC-84-EA-33-BC/FF-FF-FF-FF-FF-00". The separators can be skipped.
/DESTMAC	Specify destination MAC address as a rule. Use the same method of specification as for the /SRCMAC parameter.
/SRCIP	Specify a source IPv6 address as a rule condition. Specify the IPv6 address in the format of "IP Address/Mask" by separating the hexadecimal values using colons such as "2001:200:0:1::". For the mask, either specify hexadecimal values separated by colons such as ffff:ffff:ffff:ffff::, or you can specify the bit length from the header using a decimal value such as "64". If you specify "::/0", this means all hosts.
/DESTIP	Specify a destination IPv6 address as a rule condition in the format of "IP Address/Mask". Use the same method of specification as for the /SRCIP parameter.
/PROTOCOL	Specify a protocol type as a rule condition. Input the IP protocol number using decimal values or specify one of the keywords "tcp" (TCP/IP protocol, no.6), "udp" (UDP/IP protocol, no.17), "icmpv4" (ICMPv4 protocol, no.1), "icmpv6" (ICMPv6 protocol, no.58) or "ip" (all protocols, no.0). Specify 0 to make the rule apply to all IP protocols.
/SRCPORT	If the specified protocol is TCP/IP or UDP/IP, specify the source port number as the rule condition. Protocols other than this will be ignored. When this parameter is not specified, the rules will apply to all port numbers. When specifying, do so using the following method "1-1024" (1 to 1024), "23" (only 23).
/DESTPORT	If the specified protocol is TCP/IP or UDP/IP, specify the destination port number as the rule condition. Protocols other than this will be ignored. Use the same method of specification as for the /SRCPORT parameter.

/TCPSTATE	Specify TCP connection state as a rule. Use Established or Unestablished.

6.4.53 "AccessAddEx6": Add Extended Access List Rules (IPv6: Delay, Jitter and Packet Loss Generating)

Command Name	**AccessAddEx6**
Purpose	Add Extended Access List Rules (IPv6: Delay, Jitter and Packet Loss Generating)
Description	Use this to add a new rule to the access list of the currently managed Virtual Hub. You can set to generate delays, jitters and packet losses when a packet is passing via the Virtual Hub. The access list is a set of packet file rules that are applied to packets that flow through the Virtual Hub. You can register multiple rules in an access list and you can also define a priority for each rule. All packets are checked for the conditions specified by the rules registered in the access list and based on the operation that is stipulated by the first matching rule, they either pass or are discarded. Packets that do not match any rule are implicitly allowed to pass. You can also use the AccessAddEx6 command to generate delays, jitters and packet losses. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*AccessAddEx6 [pass|discard] [/MEMO:memo] [/PRIORITY:priority] [/SRCUSERNAME:username] [/DESTUSERNAME:username] [/SRCMAC:mac/mask] [/DESTMAC:mac/mask] [/SRCIP:ip/mask] [/DESTIP:ip/mask] [/PROTOCOL:tcp|udp|icmpv4|icmpv6|ip|num] [/SRCPORT:start-end] [/DESTPORT:start-end] [/TCPSTATE:established|unestablished] [/DELAY:delay_millisec] [/JITTER:jitter_percent] [/LOSS:loss_percent]*
Arguments for "AccessAddEx6":	
pass|discard	When a packet matches this rule condition, this operation is decided. When pass is specified, the packet is allowed to pass, and when discard is specified, the packet is discarded. The setting of delays, jitters and packet losses is applied if the action is pass.
/MEMO	Specify a description (memo) for this rule.
/PRIORITY	Specify an integer of 1 or higher to indicate the priority of the rule. Higher priority is given to rules with the lower priority values.

/SRCUSERNAME	You can apply this rule to only the packets sent by a user session of a user name that has been specified as a rule condition. In this case, specify the user name.
/DESTUSERNAME	You can apply this rule to only the packets received by a user session of a user name that has been specified as a rule condition. In this case, specify the user name.
/SRCMAC	Specify destination MAC address as a rule. Specify MAC address with "-" or ":" separators and hexadecimal number like "00-AC-84-EA-33-BC/FF-FF-FF-FF-FF-00". The separators can be skipped.
/DESTMAC	Specify destination MAC address as a rule. Use the same method of specification as for the /SRCMAC parameter.
/SRCIP	Specify a source IPv6 address as a rule condition. Specify the IPv6 address in the format of "IP Address/Mask" by separating the hexadecimal values using colons such as "2001:200:0:1::". For the mask, either specify hexadecimal values separated by colons such as "ffff:ffff:ffff:ffff::", or you can specify the bit length from the header using a decimal value such as 64. If you specify "::/0", this means all hosts.
/DESTIP	Specify a destination IPv6 address as a rule condition in the format of "IP Address/Mask". Use the same method of specification as for the /SRCIP parameter.
/PROTOCOL	Specify a protocol type as a rule condition. Input the IP protocol number using decimal values or specify one of the keywords "tcp" (TCP/IP protocol, no.6), "udp" (UDP/IP protocol, no.17), "icmpv4" (ICMPv4 protocol, no.1), "icmpv6" (ICMPv6 protocol, no.58) or "ip" (all protocols, no.0). Specify 0 to make the rule apply to all IP protocols.
/SRCPORT	If the specified protocol is TCP/IP or UDP/IP, specify the source port number as the rule condition. Protocols other than this will be ignored. When this parameter is not specified, the rules will apply to all port numbers. When specifying, do so using the following method "1-1024" (1 to 1024), "23" (only 23).
/DESTPORT	If the specified protocol is TCP/IP or UDP/IP, specify the destination port number as the rule condition. Protocols other than this will be ignored. Use the same method of specification as for the /SRCPORT parameter.
/TCPSTATE	Specify TCP connection state as a rule. Use Established or Unestablished.
/DELAY	Set this value to generate delays when packets is passing. Specify the delay period in milliseconds. Specify 0 means no delays to generate. The delays must be 10000 milliseconds at most.

/JITTER	Set this value to generate jitters when packets is passing. Specify the ratio of fluctuation of jitters within 0% to 100% range. Specify 0 means no jitters to generate.
/LOSS	Set this value to generate packet losses when packets is passing. Specify the ratio of packet losses within 0% to 100% range. Specify 0 means no packet losses to generate.

6.4.54 "AccessList": Get Access List Rule List

Command Name	**AccessList**
Purpose	Get Access List Rule List
Description	Use this to get a list of packet filter rules that are registered on access list of the currently managed Virtual Hub. The access list is a set of packet file rules that are applied to packets that flow through the Virtual Hub. You can register multiple rules in an access list and you can also define a priority for each rule. All packets are checked for the conditions specified by the rules registered in the access list and based on the operation that is stipulated by the first matching rule, they either pass or are discarded. Packets that do not match any rule are implicitly allowed to pass. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*AccessList*
Arguments for "AccessList":	
No arguments are required.	

6.4.55 "AccessDelete": Delete Rule from Access List

Command Name	**AccessDelete**
Purpose	Delete Rule from Access List
Description	Use this to specify a packet filter rule registered on the access list of the currently managed Virtual Hub and delete it. To delete a rule, you must specify that rule's ID. You can display the ID by using the AccessList command. If you wish not to delete the rule but to only temporarily disable it, use the AccessDisable command. This command cannot be run on VPN Bridge.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*AccessDelete [id]*
Arguments for "AccessDelete":	
id	Specify either the ID or the Unique ID of the rule to delete.

6.4.56 "AccessEnable": Enable Access List Rule

Command Name	**AccessEnable**
Purpose	Enable Access List Rule
Description	Use this to specify a packet filter rule registered on the access list of the currently managed Virtual Hub and enable it. The enabled rule will be used by packet filtering. To enable a rule, you must specify that rule's ID. You can display the ID by using the AccessList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*AccessEnable [id]*
Arguments for "AccessEnable":	
id	Specify the ID of the rule to enable.

6.4.57 "AccessDisable": Disable Access List Rule

Command Name	**AccessDisable**
Purpose	Disable Access List Rule
Description	Use this to specify a packet filter rule registered on the access list of the currently managed Virtual Hub and disable it. The disabled rule will be used by packet filtering. To disable a rule, you must specify that rule's ID. You can display the ID by using the AccessList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*AccessDisable [id]*
Arguments for "AccessDisable":	
id	Specify the ID of the rule to disable.

6.4.58 "UserList": Get List of Users

Command Name	**UserList**
Purpose	Get List of Users
Description	Use this to get a list of users that are registered on the security account database of the currently managed Virtual Hub. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserList*
Arguments for "UserList":	
No arguments are required.	

6.4.59 "UserCreate": Create User

Command Name	**UserCreate**
Purpose	Create User
Description	Use this to create a new user in the security account database of the currently managed Virtual Hub. By creating a user, the VPN Client can connect to the Virtual Hub by using the authentication information of that user. When a user is created using the UserCreate command and the auth type of that user is registered as Password Authentication, a random string will be assigned as the password. Therefore, that user will not be able to connect to the Virtual Hub in that state. After creating the user, you must always use the UserPasswordSet command to specify the user password, or alternatively use the UserAnonymousSet command, UserCertSet command, UserSignedSet command, UserRadiusSet command or UserNTLMSet command to change the user's auth type. Note that a user whose user name has been created as "*" (a single asterisk character) will automatically be registered as a RADIUS authentication user. For cases where there are users with "*" as the name, when a user, whose user name that was provided when a client connected to a VPN Server does not match existing user names, is able to be authenticated by a RADIUS server or NT domain controller by inputting a user name and password, the authentication settings and security policy settings will follow the setting for the user "*".

	To change the user information of a user that has been created, use the UserSet command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserCreate [name] [/GROUP:group] [/REALNAME:realname] [/NOTE:note]*
Arguments for "UserCreate":	
name	Specify the user name of the user to be newly created.
/GROUP	When assigning a user in a group, specify the group name. When not assigning a user to any group, specify /GROUP:none.
/REALNAME	Specify the user's full name. If you are not specifying this, specify /REALNAME:none.
/NOTE	Specify a description of the user. If you are not specifying this, specify /NOTE:none

6.4.60 "UserSet": Change User Information

Command Name	**UserSet**
Purpose	Change User Information
Description	Use this to change user information that is registered on the security account database of the currently managed Virtual Hub. The user information that can be changed using this command are the three items that are specified when a new user is created using the UserCreate command: Group Name, Full Name, and Description. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserSet [name] [/GROUP:group] [/REALNAME:realname] [/NOTE:note]*
Arguments for "UserSet":	
name	Specify the user name of the user whose setting you want to change.
/GROUP	When assigning a user in a group, specify the group name. When not assigning a user to any group, specify /GROUP:none.
/REALNAME	Specify the user's full name. If you are not specifying this, specify /REALNAME:none
/NOTE	Specify a description of the user. If you are not specifying this, specify /NOTE:none.

6.4.61 "UserDelete": Delete User

Command Name	**UserDelete**
Purpose	Delete User
Description	Use this to delete a user that is registered on the security account database of the currently managed Virtual Hub. By deleting the user, that user will no long be able to connect to the Virtual Hub. You can use the UserPolicySet command to instead of deleting a user, set the user to be temporarily denied from logging in. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserDelete [name]*
Arguments for "UserDelete":	
name	Specify the name of the user to delete.

6.4.62 "UserGet": Get User Information

Command Name	**UserGet**
Purpose	Get User Information
Description	Use this to get user registration information that is registered on the security account database of the currently managed Virtual Hub. The information that you can get using this command are User Name, Full Name, Group Name, Expiration Date, Security Policy, and Auth Type, as well as parameters that are specified as auth type attributes and the statistical data of that user. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserGet [name]*
Arguments for "UserGet":	
name	Specify the user name of the user whose information you want to get.

6.4.63 "UserAnonymousSet": Set Anonymous Authentication for User Auth Type

Command Name	**UserAnonymousSet**
Purpose	Set Anonymous Authentication for User Auth Type
Description	Use this to set Anonymous Authentication as the auth type for a user that is registered on the security account database of the currently managed Virtual Hub. A VPN Client that has connected to a Virtual Hub using a user name of a user set to anonymous authentication can connect to a Virtual Hub without undergoing user authentication and without conditions. The anonymous authentication function is ideally suited to public VPN Servers that are setup to allow anyone to connect via the Internet etc. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserAnonymousSet [name]*
Arguments for "UserAnonymousSet":	
name	Specify the user name of the user whose setting you want to change.

6.4.64 "UserPasswordSet": Set Password Authentication for User Auth Type and Set Password

Command Name	**UserPasswordSet**
Purpose	Set Password Authentication for User Auth Type and Set Password
Description	Use this to set Password Authentication as the auth type for a user that is registered on the security account database of the currently managed Virtual Hub. Password Authentication requires a user-defined password to be set for the user object in the security account database of the Virtual Hub and when a user attempts to connect to the Virtual Hub using this user name, they will be prompted to input a password and if it is the matching password, connection will be allowed. The user password is actually saved in hash code which means even if the VPN Server setting file is analyzed, the original password cannot be deciphered. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserPasswordSet [name] [/PASSWORD:password]*
Arguments for "UserPasswordSet":	
name	Specify the user name of the user whose setting you want to change.
/PASSWORD	Specify the password to be set for the user. If this parameter is not specified a prompt will appear to input the password.

6.4.65 "UserCertSet": Set Individual Certificate Authentication for User Auth Type and Set Certificate

Command Name	**UserCertSet**
Purpose	Set Individual Certificate Authentication for User Auth Type and Set Certificate
Description	Use this to set Individual Certificate Authentication as the Auth Type for a user that is registered on the security account database of the currently managed Virtual Hub. Individual Certificate Authentication requires one X.509 format certificate to be set for the user object in the security account database of the Virtual Hub and when a user attempts to connect to the Virtual Hub using this user name, an RSA algorithm is used to verify if the provided certificate matches the registered certificate and whether the client holds a private key that corresponds to that certificate and if so, connection is allowed. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserCertSet [name] [/LOADCERT:cert]*
Arguments for "UserCertSet":	
name	Specify the user name of the user whose setting you want to change.
/LOADCERT	Specify the certificate to set for the user by specifying an X.509 format certificate file.

6.4.66 "UserCertGet": Get Certificate Registered for Individual Certificate Authentication User

Command Name	**UserCertGet**

Purpose	Get Certificate Registered for Individual Certificate Authentication User
Description	Use this to get an X.509 format certificate registered for a user of Individual Certificate Authentication who is registered in the security account database of the currently managed Virtual Hub and save it to file. If the specified user is not set as Individual Certificate Authentication an error will occur. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserCertGet [name] [/SAVECERT:cert]*
Arguments for "UserCertGet":	
name	Specify the user name of the user whose information you want to get.
/SAVECERT	Specify the file name to save, in X.509 format, the user certificate you obtained.

6.4.67 "UserSignedSet": Set Signed Certificate Authentication for User Auth Type

Command Name	**UserSignedSet**
Purpose	Set Signed Certificate Authentication for User Auth Type
Description	Use this to set Signed Certificate Authentication as the auth type for a user that is registered on the security account database of the currently managed Virtual Hub. When a user connects to a Virtual Hub using a user name that is set for signed certificate authentication, an RSA algorithm is used to verify whether the certificate provided by the user is signed by any of the certificates in the list of trusted CA certificates of that Virtual Hub and whether the client holds a private key that corresponds with that certificate, and if so, connection is allowed. It is also possible to set the connection to be allowed only when a certificate common name (CN) and serial number that is expected for each user is registered and the contents of the certificate after the abovementioned verification is passed matches the set value. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserSignedSet [name] [/CN:cn] [/SERIAL:serial]*
Arguments for "UserSignedSet":	
name	Specify the user name of the user whose setting you want to change.
/CN	When this parameter is set, after it has been verified that the certificate that the user provided has been signed by the trusted certificate authority, connection will only be allowed when the value of the common name (CN) of this certificate is compared with the value set by this parameter and the values match. When "none" is specified, this check is not made.
/SERIAL	When this parameter is set, after it has been verified that the certificate that the user provided has been signed by the trusted certificate authority, connection will only be allowed when the value of the serial number of this certificate is compared with the value set by this parameter and the values match. When "none" is specified, this check is not made.

6.4.68 "UserRadiusSet": Set RADIUS Authentication for User Auth Type

Command Name	**UserRadiusSet**
Purpose	Set RADIUS Authentication for User Auth Type
Description	Use this to set RADIUS Authentication as the auth type for a user that is registered on the security account database of the currently managed Virtual Hub. When a user connects to a Virtual Hub using a user name that is set for RADIUS authentication, the user name and the user input password is sent to the RADIUS server where the RADIUS SERVER checks the user name and password, then if the verification is successful, that user is allowed VPN connection. In order to user RADIUS authentication, the RADIUS server used for this verification must be set in the Virtual Hub beforehand by using the RadiusServerSet command. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserRadiusSet [name] [/ALIAS:alias_name]*
Arguments for "UserRadiusSet":	
name	Specify the user name of the user whose setting you want to change.

/ALIAS	When this parameter is set, it is possible to make the user name sent to the RADIUS server different to the user name on the Virtual Hub. When this is not set, please specify /ALIAS:none (the user name on the Virtual Hub will be used). If the user name is "*", the /ALIAS parameter will be ignored. To read an explanation of the "*" user, please input UserCreate/HELP to display this information.

6.4.69 "UserNTLMSet": Set NT Domain Authentication for User Auth Type

Command Name	**UserNTLMSet**
Purpose	Set NT Domain Authentication for User Auth Type
Description	Use this to set NT Domain Authentication as the auth type for a user that is registered on the security account database of the currently managed Virtual Hub. When a user connects to a Virtual Hub using a user name that is set for NT Domain authentication, the user name and the user input password is sent to the Windows NT / 2000 / Server 2003 / Server 2008 / Server 2008 R2 / Server 2012 Domain Controller or Active Directory Server where the server checks the user name and password, then if the verification is successful, that user is allowed VPN connection. To use NT Domain authentication, the VPN Server must be operating on a Windows NT 4.0, Windows 2000, Windows XP, Windows Vista, Windows Server 2008, Windows Server 2008 R2 or Windows Server 2012 operating system that is connected to that domain. For details please contact the VPN Server's administrator. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserNTLMSet [name] [/ALIAS:alias_name]*
Arguments for "UserNTLMSet":	
name	Specify the user name of the user whose setting you want to change.
/ALIAS	When this parameter is set, it is possible to make the user name sent to the NT Domain or Active Directory server different to the user name on the Virtual Hub. When this is not set, please specify /ALIAS:none (the user name on the Virtual Hub will be used). If the user name is "*", the /ALIAS parameter will be ignored. To read an explanation of the "*" user, please input UserCreate/HELP to display this information.

6.4.70 "UserPolicyRemove": Delete User Security Policy

Command Name	**UserPolicyRemove**
Purpose	Delete User Security Policy
Description	Use this to delete the security policy setting that is set for a user that is registered on the security account database of the currently managed Virtual Hub. A user who has had their security policy setting deleted will be assigned the security policy setting of the group that user is assigned to. In the cases where the user is not assigned to a group or when a security policy setting has not been set for the group, the default values (Allow Access: Enabled, Maximum Number of TCP Connections: 32, Time-out Period: 20 seconds) will be applied. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserPolicyRemove [name]*
Arguments for "UserPolicyRemove":	
name	Specify the user name of the user whose setting you want to change.

6.4.71 "UserPolicySet": Set User Security Policy

Command Name	**UserPolicySet**
Purpose	Set User Security Policy
Description	Use this to set the security policy contents that are set for a user that is registered on the security account database of the currently managed Virtual Hub. When a user has not been set a security policy, use this to change the specified values after a new default security policy has been set. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserPolicySet [name] [/NAME:policy_name] [/VALUE:num|yes|no]*
Arguments for "UserPolicySet":	
name	Specify the user name of the user whose setting you want to change.

/NAME	Specify the name of policy whose values you want to change. You can use the PolicyList command to display a list of policy names and values that can be set.
/VALUE	Specify a new policy value. If the policy is an integer value, specify an integer. Specify yes or no for Boolean types. You can view the type and value that can be set by using the PolicyList command.

6.4.72 "UserExpiresSet": Set User's Expiration Date

Command Name	**UserExpiresSet**
Purpose	Set User's Expiration Date
Description	Use this to set the user's expiration date that is registered on the security account database of the currently managed Virtual Hub. A user whose expiration date has expired cannot connect to the Virtual Hub. To get the list of currently registered users, use the UserList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*UserExpiresSet [name] [/EXPIRES:expires]*
Arguments for "UserExpiresSet":	
name	Specify the user name of the user whose setting you want to change.
/EXPIRES	Specify the user expiration date and time. The date and time must be in the same format as "2005/10/08 19:30:00" where 6 integers are specified, representing year/month/day hour:minute:second separated by forward slashes, a space and then colons. Specify 4 digits for the year. If you put a space in a value, the entire value must be enclosed by "". For this specification, local time (standard time for the computer on which the command line management utility is running) can be specified. By specifying /EXPIRES:none, you can remove the expiration date restriction.

6.4.73 "GroupList": Get List of Groups

Command Name	**GroupList**
Purpose	Get List of Groups
Description	Use this to get a list of groups that are registered on the security account database of the currently managed Virtual Hub.

	This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*GroupList*
Arguments for "GroupList":	
No arguments are required.	

6.4.74 "GroupCreate": Create Group

Command Name	**GroupCreate**
Purpose	Create Group
Description	Use this to create a new group in the security account database of the currently managed Virtual Hub. You can register multiple users in a group. To register users in a group use the GroupJoin command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*GroupCreate [name] [/REALNAME:realname] [/NOTE:note]*
Arguments for "GroupCreate":	
name	Specify the name of the group to create.
/REALNAME	Specify the group's full name. For example, if the group corresponds to an actual section or department name, specify that name. If you are not specifying this, specify /REALNAME:none
/NOTE	Specify a description of the group. If you are not specifying this, specify /NOTE:none

6.4.75 "GroupSet": Set Group Information

Command Name	**GroupSet**
Purpose	Set Group Information
Description	Use this to set group information that is registered on the security account database of the currently managed Virtual Hub. To get the list of currently registered groups, use the GroupList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.

Command-line	*GroupSet [name] [/REALNAME:realname] [/NOTE:note]*
Arguments for "GroupSet":	
name	Specify the group name of the group whose setting you want to change.
/REALNAME	Specify the group's Full name. For example, if the group corresponds to an actual section or department name, specify that name. If you are not specifying this, specify /REALNAME:none
/NOTE	Specify a description of the group. If you are not specifying this, specify /NOTE:none.

6.4.76 "GroupDelete": Delete Group

Command Name	**GroupDelete**
Purpose	Delete Group
Description	Use this to delete a group that is registered on the security account database of the currently managed Virtual Hub. When you delete a group all users assigned to that group will become unassigned. To get the list of currently registered groups, use the GroupList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*GroupDelete [name]*
Arguments for "GroupDelete":	
name	Specify the name of the group to delete.

6.4.77 "GroupGet": Get Group Information and List of Assigned Users

Command Name	**GroupGet**
Purpose	Get Group Information and List of Assigned Users
Description	Use this to get the information of a group that is registered on the security account database of the currently managed Virtual Hub as well as a list of users assigned to that group. To get the list of currently registered groups, use the GroupList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.

Command-line	*GroupGet [name]*
Arguments for "GroupGet":	
name	Specify the group name of the group whose information you want to get.

6.4.78 "GroupJoin": Add User to Group

Command Name	**GroupJoin**
Purpose	Add User to Group
Description	Use this to add a user in the security account database of the currently managed Virtual Hub to a group that is registered on that security account database. To get a list of users and groups that are currently registered, use the UserList command and the GroupList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*GroupJoin [name] [/USERNAME:username]*
Arguments for "GroupJoin":	
name	Specify the group name of the group to which you want to add a user.
/USERNAME	Specify the user name of the user you want to add to the group specified by "name".

6.4.79 "GroupUnjoin": Delete User from Group

Command Name	**GroupUnjoin**
Purpose	Delete User from Group
Description	Use this to delete a specified user from the group that is registered on the security account database of the currently managed Virtual Hub. By deleting a user from the group, that user becomes unassigned. To get a list of users that are currently assigned to a group, use the GroupGet command. To get the list of currently registered groups, use the GroupList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*GroupUnjoin [name]*
Arguments for "GroupUnjoin":	

name	Specify the name of the user to delete from the group.

6.4.80 "GroupPolicyRemove": Delete Group Security Policy

Command Name	**GroupPolicyRemove**
Purpose	Delete Group Security Policy
Description	Use this to delete the security policy setting that is set for a group that is registered on the security account database of the currently managed Virtual Hub. Users who do not have a security policy set for the user themselves or for the group they are assigned to, will have the default values (Allow Access: Enabled, Maximum Number of TCP Connections: 32, Time-out Period: 20 seconds) applied to them. To get the list of currently registered groups, use the GroupList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*GroupPolicyRemove [name]*
Arguments for "GroupPolicyRemove":	
name	Specify the group name of the group whose setting you want to change.

6.4.81 "GroupPolicySet": Set Group Security Policy

Command Name	**GroupPolicySet**
Purpose	Set Group Security Policy
Description	Use this to set the security policy contents that are set for a group that is registered on the security account database of the currently managed Virtual Hub. When a group has not been set a security policy, use this to change the specified values after a new default security policy has been set. To get the list of currently registered groups, use the GroupList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a member server on a cluster.
Command-line	*GroupPolicySet [name] [/NAME:policy_name] [/VALUE:num|yes|no]*
Arguments for "GroupPolicySet":	

name	Specify the group name of the group whose setting you want to change.
/NAME	Specify the name of policy whose values you want to change. You can use the PolicyList command to display a list of policy names and values that can be set.
/VALUE	Specify a new policy value. If the policy is an integer value, specify an integer. Specify yes or no for Boolean types. You can view the type and value that can be set by using the PolicyList command.

6.4.82 "SessionList": Get List of Connected Sessions

Command Name	**SessionList**
Purpose	Get List of Connected Sessions
Description	Use this to get a list of the sessions connected to the Virtual Hub currently being managed. In the list of sessions, the following information will be displayed for each connection: Session Name, Session Site, User Name, Source Host Name, TCP Connection, Transfer Bytes and Transfer Packets. If the currently connected VPN Server is a cluster controller and the currently managed Virtual Hub is a static Virtual Hub, you can get an all-linked-together list of all sessions connected to that Virtual Hub on all cluster members. In all other cases, only the list of sessions that are actually connected to the currently managed VPN Server will be obtained.
Command-line	*SessionList*
Arguments for "SessionList":	
No arguments are required.	

6.4.83 "SessionGet": Get Session Information

Command Name	**SessionGet**
Purpose	Get Session Information
Description	Use this to specify a session currently connected to the currently managed Virtual Hub and get the session information. The session information includes the following: source host name and user name, version information, time information, number of TCP connections, communication parameters, session key, statistical information on data transferred, and other client and server information.

	To get the list of currently connected sessions, use the SessionList command.
Command-line	*SessionGet [name]*
Arguments for "SessionGet":	
name	Specify the session name of the session whose information you want to get.

6.4.84 "SessionDisconnect": Disconnect Session

Command Name	**SessionDisconnect**
Purpose	Disconnect Session
Description	Use this to specify a session currently connected to the currently managed Virtual Hub and forcefully disconnect that session using manager privileges. Note that when communication is disconnected by settings on the source client side and the automatically reconnect option is enabled, it is possible that the client will reconnect. To get the list of currently connected sessions, use the SessionList command.
Command-line	*SessionDisconnect [name]*
Arguments for "SessionDisconnect":	
name	Specify the session name of the session to disconnect.

6.4.85 "MacTable": Get the MAC Address Table Database

Command Name	**MacTable**
Purpose	Get the MAC Address Table Database
Description	Use this to get the MAC address table database that is held by the currently managed Virtual Hub. The MAC address table database is a table that the Virtual Hub requires to perform the action of switching Ethernet frames and the Virtual Hub decides the sorting destination session of each Ethernet frame based on the MAC address table database. The MAC address database is built by the Virtual Hub automatically analyzing the contents of the communication throughput. By specifying the session name you can get the MAC address table entry that has been associated with that session.
Command-line	*MacTable [session_name]*
Arguments for "MacTable":	

session_name	By specifying the session name as a parameter, you can display only the MAC address table entry that is associated with that session. When this is left unspecified, all the entries will be displayed.

6.4.86 "MacDelete": Delete MAC Address Table Entry

Command Name	**MacDelete**
Purpose	Delete MAC Address Table Entry
Description	Use this command to operate the MAC address table database held by the currently managed Virtual Hub and delete a specified MAC address table entry from the database. To get the contents of the current MAC address table database use the MacTable command.
Command-line	*MacDelete [id]*
Arguments for "MacDelete":	
id	Specify the ID of the MAC address table entry to delete.

6.4.87 "IpTable": Get the IP Address Table Database

Command Name	**IpTable**
Purpose	Get the IP Address Table Database
Description	Use this to get the IP address table database that is held by the currently managed Virtual Hub. The IP address table database is a table that is automatically generated by analyzing the contents of communication so that the Virtual Hub can always know which session is using which IP address and it is frequently used by the engine that applies the Virtual Hub security policy. By specifying the session name you can get the IP address table entry that has been associated with that session.
Command-line	*IpTable [session_name]*
Arguments for "IpTable":	
session_name	By specifying the session name as a parameter, you can display only the IP address table entry that is associated with that session. When this is left unspecified, all the entries will be displayed.

6.4.88 "IpDelete": Delete IP Address Table Entry

Command Name	**IpDelete**
Purpose	Delete IP Address Table Entry
Description	Use this command to operate the IP address table database held by the currently managed Virtual Hub and delete a specified IP address table entry from the database. To get the contents of the current IP address table database use the IpTable command.
Command-line	*IpDelete [id]*
Arguments for "IpDelete":	
id	Specify the ID of the IP address table entry to delete.

6.4.89 "SecureNatEnable": Enable the Virtual NAT and DHCP Server Function (SecureNat Function)

Command Name	**SecureNatEnable**
Purpose	Enable the Virtual NAT and DHCP Server Function (SecureNat Function)
Description	Use this to enable the Virtual NAT and DHCP Server function (SecureNat Function) on the currently managed Virtual Hub and begin its operation. Before executing this command, you must first check the setting contents of the current Virtual NAT function and DHCP Server function using the SecureNatHostGet command, NatGet command and DhcpGet command. By enabling the SecureNAT function, you can virtually operate a NAT router (IP masquerade) and the DHCP Server function on a virtual network on the Virtual Hub. [Warning about SecureNAT Function] The SecureNAT function is recommended only for system administrators and people with a detailed knowledge of networks. If you use the SecureNAT function correctly, it is possible to achieve a safe form of remote access via a VPN. However when used in the wrong way, it can put the entire network in danger. Anyone who does not have a thorough knowledge of networks and anyone who does not have the network administrator's permission must not enable the SecureNAT function. For a detailed explanation of the SecureNAT function, please refer to the VPN Server's manual and online documentation.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SecureNatEnable*
Arguments for "SecureNatEnable":	
No arguments are required.	

6.4.90 "SecureNatDisable": Disable the Virtual NAT and DHCP Server Function (SecureNat Function)

Command Name	**SecureNatDisable**
Purpose	Disable the Virtual NAT and DHCP Server Function (SecureNat Function)
Description	Use this to disable the Virtual NAT and DHCP Server function (SecureNat Function) on the currently managed Virtual Hub. By executing this command the Virtual NAT function immediately stops operating and the Virtual DHCP Server function deletes the DHCP lease database and stops the service. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SecureNatDisable*
Arguments for "SecureNatDisable":	
No arguments are required.	

6.4.91 "SecureNatStatusGet": Get the Operating Status of the Virtual NAT and DHCP Server Function (SecureNat Function)

Command Name	**SecureNatStatusGet**
Purpose	Get the Operating Status of the Virtual NAT and DHCP Server Function (SecureNat Function)
Description	Use this to get the operating status of the Virtual NAT and DHCP Server function (SecureNat Function) when it is operating on the currently managed Virtual Hub. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SecureNatStatusGet*
Arguments for "SecureNatStatusGet":	
No arguments are required.	

6.4.92 "SecureNatHostGet": Get Network Interface Setting of Virtual Host of SecureNAT Function

Command Name	**SecureNatHostGet**
Purpose	Get Network Interface Setting of Virtual Host of SecureNAT Function
Description	Use this to get the virtual host network interface setting from the setting items of the Virtual NAT and DHCP Server function (SecureNAT function) on the currently managed Virtual Hub. The SecureNAT function holds one virtual network adapter on the L2 segment inside the Virtual Hub and it has been assigned a MAC address and an IP address. By doing this, another host connected to the same L2 segment is able to communicate with the SecureNAT virtual host as if it is an actual IP host existing on the network. [Warning about SecureNAT Function] The SecureNAT function is recommended only for system administrators and people with a detailed knowledge of networks. If you use the SecureNAT function correctly, it is possible to achieve a safe form of remote access via a VPN. However when used in the wrong way, it can put the entire network in danger. Anyone who does not have a thorough knowledge of networks and anyone who does not have the network administrators permission must not enable the SecureNAT function. For a detailed explanation of the SecureNAT function, please refer to the VPN Server's manual and online documentation. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SecureNatHostGet*
Arguments for "SecureNatHostGet":	
No arguments are required.	

6.4.93 "SecureNatHostSet": Change Network Interface Setting of Virtual Host of SecureNAT Function

Command Name	**SecureNatHostSet**
Purpose	Change Network Interface Setting of Virtual Host of SecureNAT Function

Description	Use this to change and save the virtual host network interface setting in the setting items of the Virtual NAT and DHCP Server function (SecureNAT function) on the currently managed Virtual Hub. The SecureNAT function holds one virtual network adapter on the L2 segment inside the Virtual Hub and it has been assigned a MAC address and an IP address. By doing this, another host connected to the same L2 segment is able to communicate with the SecureNAT virtual host as if it is an actual IP host existing on the network. [Warning about SecureNAT Function] The SecureNAT function is recommended only for system administrators and people with a detailed knowledge of networks. If you use the SecureNAT function correctly, it is possible to achieve a safe form of remote access via a VPN. However when used in the wrong way, it can put the entire network in danger. Anyone who does not have a thorough knowledge of networks and anyone who does not have the network administrators permission must not enable the SecureNAT function. For a detailed explanation of the SecureNAT function, please refer to the VPN Server's manual and online documentation. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*SecureNatHostSet [/MAC:mac] [/IP:ip] [/MASK:mask]*
Arguments for "SecureNatHostSet":	
/MAC	Specify the MAC address to assign for the virtual interface. Specify a MAC address using a string like "00-AC-01-23-45-67". When /MAC:none is specified, no changes will be made to the current setting.
/IP	Specify the IP address to assign for the virtual interface. When /IP:none is specified, no changes will be made to the current setting.
/MASK	Specify the subnet mask to assign for the virtual interface. When /MASK:none is specified, no changes will be made to the current setting.

6.4.94 "NatGet": Get Virtual NAT Function Setting of SecureNAT Function

Command Name	**NatGet**
Purpose	Get Virtual NAT Function Setting of SecureNAT Function
Description	Use this to get the virtual NAT setting from the setting items of the Virtual NAT and DHCP Server function (SecureNAT function) on

	the currently managed Virtual Hub. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*NatGet*
Arguments for "NatGet":	
No arguments are required.	

6.4.95 "NatEnable": Enable Virtual NAT Function of SecureNAT Function

Command Name	**NatEnable**
Purpose	Enable Virtual NAT Function of SecureNAT Function
Description	Use this to enable the Virtual NAT function on the currently managed Virtual Hub. If the SecureNAT function is still not operating even after this command has been used to enable the Virtual NAT function, Virtual NAT is not operating. To start the operation of the SecureNAT Function, use the SecureNatEnable command. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*NatEnable*
Arguments for "NatEnable":	
No arguments are required.	

6.4.96 "NatDisable": Disable Virtual NAT Function of SecureNAT Function

Command Name	**NatDisable**
Purpose	Disable Virtual NAT Function of SecureNAT Function
Description	Use this to disable the Virtual NAT function on the currently managed Virtual Hub. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*NatDisable*
Arguments for "NatDisable":	
No arguments are required.	

6.4.97 "NatSet": Change Virtual NAT Function Setting of SecureNAT Function

Command Name	**NatSet**
Purpose	Change Virtual NAT Function Setting of SecureNAT Function
Description	Use this to change the Virtual NAT setting of the currently managed Virtual Hub. The contents of the Virtual NAT setting includes: MTU value, TCP session timeout and UDP session timeout You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*NatSet [/MTU:mtu] [/TCPTIMEOUT:tcp_timeout] [/UDPTIMEOUT:udp_timeout] [/LOG:yes|no]*
Arguments for "NatSet":	
/MTU	Set the MTU (Maximum transferable unit size) using an integer to specify the byte length unit. This value is the maximum payload length excluding the MAC header of the Ethernet frame that the Virtual NAT sends and the default is 1500 bytes.
/TCPTIMEOUT	This sets how many seconds a condition of non-communication continues in a TCP session that the Virtual NAT is relaying before a timeout occurs and the session is discarded.
/UDPTIMEOUT	This sets how many seconds a condition of non-communication continues in a UDP session that the Virtual NAT is relaying before a timeout occurs and the session is discarded.
/LOG	Specify whether or not to save the Virtual NAT operation in the Virtual Hub security log. Specify "yes" to save it, and "no" to not save it.

6.4.98 "NatTable": Get Virtual NAT Function Session Table of SecureNAT Function

Command Name	**NatTable**
Purpose	Get Virtual NAT Function Session Table of SecureNAT Function
Description	Use this to get the table of TCP and UDP sessions currently communicating via the Virtual NAT (NAT table) in cases when the Virtual NAT function is operating on the currently managed Virtual Hub. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*NatTable*
Arguments for "NatTable":	

No arguments are required.

6.4.99 "DhcpGet": Get Virtual DHCP Server Function Setting of SecureNAT Function

Command Name	**DhcpGet**
Purpose	Get Virtual DHCP Server Function Setting of SecureNAT Function
Description	Use this to get the virtual DHCP Server setting from the setting items of the Virtual NAT and DHCP Server function (SecureNAT function) on the currently managed Virtual Hub. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*DhcpGet*
Arguments for "DhcpGet":	
No arguments are required.	

6.4.100 "DhcpEnable": Enable Virtual DHCP Server Function of SecureNAT Function

Command Name	**DhcpEnable**
Purpose	Enable Virtual DHCP Server Function of SecureNAT Function
Description	Use this to enable the Virtual DHCP Server function on the currently managed Virtual Hub. If the SecureNAT function is still not operating even after this command has been used to enable the Virtual DHCP function, Virtual DHCP Server is not operating. To start the operation of the SecureNAT Function, use the SecureNatEnable command. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*DhcpEnable*
Arguments for "DhcpEnable":	
No arguments are required.	

6.4.101 "DhcpDisable": Disable Virtual DHCP Server Function of SecureNAT Function

Command Name	**DhcpDisable**
Purpose	Disable Virtual DHCP Server Function of SecureNAT Function
Description	Use this to disable the Virtual DHCP Server function on the currently managed Virtual Hub. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*DhcpDisable*
Arguments for "DhcpDisable":	
No arguments are required.	

6.4.102 "DhcpSet": Change Virtual DHCP Server Function Setting of SecureNAT Function

Command Name	**DhcpSet**
Purpose	Change Virtual DHCP Server Function Setting of SecureNAT Function
Description	Use this to change the Virtual DHCP Server setting of the currently managed Virtual Hub. The Virtual DHCP Server settings include the following items: distribution address band, subnet mask, lease limit, and option values assigned to clients. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*DhcpSet [/START:start_ip] [/END:end_ip] [/MASK:subnetmask] [/EXPIRE:sec] [/GW:gwip] [/DNS:dns] [/DNS2:dns2][/ DOMAIN:domain] [/LOG:yes|no]*
Arguments for "DhcpSet":	
/START	Specify the start point of the address band to be distributed to the client. (Example: 192.168.30.10)
/END	Specify the end point of the address band to be distributed to the client. (Example: 192.168.30.200)
/MASK	Specify the subnet mask to be specified for the client. (Example: 255.255.255.0)
/EXPIRE	Specify the expiration date in second units for leasing an IP address to a client.
/GW	Specify the IP address of the default gateway to be notified to the client. You can specify a SecureNAT Virtual Host IP address for this when the SecureNAT Function's Virtual NAT Function has been

	enabled and is being used also. If you specify 0 or none, then the client will not be notified of the default gateway.
/DNS	Specify the IP address of the primary DNS Server to be notified to the client. You can specify a SecureNAT Virtual Host IP address for this when the SecureNAT Function's Virtual NAT Function has been enabled and is being used also. If you specify 0 or none, then the client will not be notified of the DNS Server address.
/DOMAIN	Specify the domain name to be notified to the client. If you specify none, then the client will not be notified of the domain name.
/LOG	Specify whether or not to save the Virtual DHCP Server operation in the Virtual Hub security log. Specify "yes" to save it. This value is interlinked with the Virtual NAT Function log save setting.

6.4.103 "DhcpTable": Get Virtual DHCP Server Function Lease Table of SecureNAT Function

Command Name	**DhcpTable**
Purpose	Get Virtual DHCP Server Function Lease Table of SecureNAT Function
Description	Use this to get the lease table of IP addresses, held by the Virtual DHCP Server, that are assigned to clients in cases when the Virtual NAT function is operating on the currently managed Virtual Hub. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*DhcpTable*
Arguments for "DhcpTable":	
No arguments are required.	

6.4.104 "AdminOptionList": Get List of Virtual Hub Administration Options

Command Name	**AdminOptionList**
Purpose	Get List of Virtual Hub Administration Options
Description	Use this to get a list of Virtual Hub administration options that are set on the currently managed Virtual Hub. The purpose of the Virtual Hub administration options is for the VPN Server Administrator to set limits for the setting ranges when the administration of the Virtual Hub is to be trusted to each Virtual Hub

	administrator. Only an administrator with administration privileges for this entire VPN Server is able to add, edit and delete the Virtual Hub administration options. The Virtual Hub administrators are unable to make changes to the administration options, however they are able to view them. There is an exception however. If allow_hub_admin_change_option is set to "1", even Virtual Hub administrators are able to edit the administration options. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster member.
Command-line	*AdminOptionList*
Arguments for "AdminOptionList":	
No arguments are required.	

6.4.105 "AdminOptionSet": Set Values of Virtual Hub Administration Options

Command Name	**AdminOptionSet**
Purpose	Set Values of Virtual Hub Administration Options
Description	Use this to change the values of Virtual Hub administration options that are set on the currently managed Virtual Hub. The purpose of the Virtual Hub administration options is for the VPN Server Administrator to set limits for the setting ranges when the administration of the Virtual Hub is to be trusted to each Virtual Hub administrator. Only an administrator with administration privileges for this entire VPN Server is able to add, edit and delete the Virtual Hub administration options. The Virtual Hub administrators are unable to make changes to the administration options, however they are able to view them. There is an exception however. If allow_hub_admin_change_option is set to "1", even Virtual Hub administrators are able to edit the administration options. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster member.
Command-line	*AdminOptionSet [name] [/VALUE:value]*
Arguments for "AdminOptionSet":	

name	Specify the name of the administration option whose value you want to change. You can get a list of names by using the AdminOptionList command.
/VALUE	Specify an integer for the setting value.

6.4.106 "ExtOptionList": Get List of Virtual Hub Extended Options

Command Name	**ExtOptionList**
Purpose	Get List of Virtual Hub Extended Options
Description	Use this to get a Virtual Hub Extended Options List that is set on the currently managed Virtual Hub. Virtual Hub Extended Option enables you to configure more detail settings of the Virtual Hub. By default, both VPN Server's global administrators and individual Virtual Hub's administrators can modify the Virtual Hub Extended Options. However, if the deny_hub_admin_change_ext_option is set to 1 on the Virtual Hub Admin Options, the individual Virtual Hub's administrators cannot modify the Virtual Hub Extended Options. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster member.
Command-line	*ExtOptionList*
Arguments for "ExtOptionList":	
No arguments are required.	

6.4.107 "ExtOptionSet": Set a Value of Virtual Hub Extended Options

Command Name	**ExtOptionSet**
Purpose	Set a Value of Virtual Hub Extended Options
Description	Use this to set a value in the Virtual Hub Extended Options List that is set on the currently managed Virtual Hub. Virtual Hub Extended Option enables you to configure more detail settings of the Virtual Hub. By default, both VPN Server's global administrators and individual Virtual Hub's administrators can modify the Virtual Hub Extended Options. However, if the deny_hub_admin_change_ext_option is set to 1 on the Virtual Hub Admin Options, the individual Virtual Hub's

	administrators cannot modify the Virtual Hub Extended Options. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster member.
Command-line	*ExtOptionSet [name] [/VALUE:value]*
Arguments for "ExtOptionSet":	
name	Specify the name of the Virtual Hub Extended Options whose value you want to change. You can get a list of names by using the ExtOptionList command.
/VALUE	Specify an integer for the setting value.

6.4.108 "CrlList": Get List of Certificates Revocation List

Command Name	**CrlList**
Purpose	Get List of Certificates Revocation List
Description	Use this to get a Certificates Revocation List that is set on the currently managed Virtual Hub. By registering certificates in the Certificates Revocation List, the clients who provide these certificates will be unable to connect to this Virtual Hub using certificate authentication mode. Normally with this function, in cases where the security of a private key has been compromised or where a person holding a certificate has been stripped of their privileges, by registering that certificate as invalid on the Virtual Hub, it is possible to deny user authentication when that certificate is used by a client to connect to the Virtual Hub. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CrlList*
Arguments for "CrlList":	
No arguments are required.	

6.4.109 "CrlAdd": Add a Revoked Certificate

Command Name	**CrlAdd**
Purpose	Add a Revoked Certificate
Description	Use this to add a new revoked certificate definition in the Certificate Revocation List that is set on the currently managed Virtual Hub. Specify the contents to be registered in the Certificate Revocation

	List by using the parameters of this command. When a user connects to a Virtual Hub in certificate authentication mode and that certificate matches 1 or more of the contents registered in the certificates revocation list, the user is denied connection. A certificate that matches all the conditions that are defined by the parameters specified by this command will be judged as invalid. The items that can be set are as follows: Name (CN), Organization (O), Organization Unit (OU), Country (C), State (ST), Locale (L), Serial Number (hexadecimal), MD5 Digest Value (hexadecimal, 128 bit), and SHA-1 Digest Value (hexadecimal, 160 bit). For the specification of a digest value (hash value) a certificate is optionally specified depending on the circumstances. Normally when a MD5 or SHA-1 digest value is input, it is not necessary to input the other items. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CrlAdd [/SERIAL:serial] [/MD5:md5] [/SHA1:sha1] [/CN:cn] [/O:o] [/OU:ou] [/C:c] [/ST:st] [/L:l]*
Arguments for "CrlAdd":	
/SERIAL	Use this parameter to specify the value for the certificate serial number (hexadecimal) when it is set as a condition.
/MD5	Use this parameter to specify the value for the certificate MD5 digest value (hexadecimal, 128 bits) when it is set as a condition. If this parameter specification is other than a hexadecimal value of 32 characters (16 bytes), it will be ignored.
/SHA1	Use this parameter to specify the value for the certificate SHA1 digest value (hexadecimal, 160 bits) when it is set as a condition. If this parameter specification is other than a hexadecimal value of 40 characters (16 bytes), it will be ignored.
/CN	Use this parameter to specify the name (CN) of the certificate when it is set as a condition.
/O	Use this parameter to specify the organization (O) of the certificate when it is set as a condition.
/OU	Use this parameter to specify the organization unit (OU) of the certificate when it is set as a condition.
/C	Use this parameter to specify the country (C) of the certificate when it is set as a condition.
/ST	Use this parameter to specify the state (ST) of the certificate when it is set as a condition.
/L	Use this parameter to specify the locale (L) of the certificate when it is set as a condition.

6.4.110 "CrlDel": Delete a Revoked Certificate

Command Name	**CrlDel**
Purpose	Delete a Revoked Certificate
Description	Use this to specify and delete a revoked certificate definition from the certificate revocation list that is set on the currently managed Virtual Hub. To get the list of currently registered revoked certificate definitions, use the CrlList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CrlDel [id]*
Arguments for "CrlDel":	
id	Specify the ID of the revoked certificate definition you want to delete.

6.4.111 "CrlGet": Get a Revoked Certificate

Command Name	**CrlGet**
Purpose	Get a Revoked Certificate
Description	Use this to specify and get the contents of a revoked certificate definition from the Certificates Revocation List that is set on the currently managed Virtual Hub. To get the list of currently registered revoked certificate definitions, use the CrlList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*CrlGet [id]*
Arguments for "CrlGet":	
id	Specify the ID of the revoked certificate definition you want to get.

6.4.112 "AcList": Get List of Rule Items of Source IP Address Limit List

Command Name	**AcList**
Purpose	Get List of Rule Items of Source IP Address Limit List
Description	Use this to get a list of Source IP Address Limit List rules that is set on the currently managed Virtual Hub. You can allow or deny VPN connections to this Virtual Hub according to the client computer's source IP address. You can define multiple rules and set a priority for each rule. The search proceeds from the rule with the highest order or priority and based on the action of the rule that the IP address first matches, the connection from the client is either allowed or denied. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*AcList*
Arguments for "AcList":	
No arguments are required.	

6.4.113 "AcAdd": Add Rule to Source IP Address Limit List (IPv4)

Command Name	**AcAdd**
Purpose	Add Rule to Source IP Address Limit List (IPv4)
Description	Use this to add a new rule to the Source IP Address Limit List that is set on the currently managed Virtual Hub. The items set here will be used to decide whether to allow or deny connection from a VPN Client when this client attempts connection to the Virtual Hub. You can specify a client IP address, or IP address or mask to match the rule as the contents of the rule item. By specifying an IP address only, there will only be one specified computer that will match the rule, but by specifying an IP net mask address or subnet mask address, all the computers in the range of that subnet will match the rule. You can specify the priority for the rule. You can specify an integer of 1 or greater for the priority and the smaller the number, the higher the priority. To get a list of the currently registered Source IP Address Limit List, use the AcList command. This command cannot be run on VPN Bridge.

	You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*AcAdd [allow|deny] [/PRIORITY:priority] [/IP:ip/mask]*
Arguments for "AcAdd":	
allow|deny	Set whether to "allow" or "deny" the connection from a client that matches the rule.
/PRIORITY	Specify an integer of 1 or higher to indicate the priority of the rule. The smaller the value the higher the priority.
/IP	Using the format: "IP Address/Mask", specify the range of client IPv4 addresses. Specify the IPv4 address by separating the decimal values using dots such as "192.168.0.1". For the mask, either specify decimal values separated by dots such as "255.255.255.0", or you can specify the bit length from the header using a decimal value such as "24". To specify a single IPv4 host, specify the mask as "32" or "255.255.255.255".

6.4.114 "AcDel": Delete Rule from Source IP Address Limit List

Command Name	**AcDel**
Purpose	Delete Rule from Source IP Address Limit List
Description	Use this to delete a rule from the Source IP Address Limit List that is set on the currently managed Virtual Hub. To get a list of the currently registered IP access control list, use the AcList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*AcDel [id]*
Arguments for "AcDel":	
id	Specify the ID of the rule in the Source IP Address Limit List that you want to delete.

6.4.115 "AcAdd6": Add Rule to Source IP Address Limit List (IPv6)

Command Name	**AcAdd6**
Purpose	Add Rule to Source IP Address Limit List (IPv6)
Description	Use this to add a new rule to the Source IP Address Limit List that is set on the currently managed Virtual Hub. The items set here will be used to decide whether to allow or deny

	connection from a VPN Client when this client attempts connection to the Virtual Hub. You can specify a client IP address, or IP address or mask to match the rule as the contents of the rule item. By specifying an IP address only, there will only be one specified computer that will match the rule, but by specifying an IP net mask address or subnet mask address, all the computers in the range of that subnet will match the rule. You can specify the priority for the rule. You can specify an integer of 1 or greater for the priority and the smaller the number, the higher the priority. To get a list of the currently registered Source IP Address Limit List, use the AcList command. This command cannot be run on VPN Bridge. You cannot execute this command for Virtual Hubs of VPN Servers operating as a cluster.
Command-line	*AcAdd6 [allow|deny] [/PRIORITY:priority] [/IP:ip/mask]*
Arguments for "AcAdd6":	
allow|deny	Set whether to "allow" or "deny" the connection from a client that matches the rule.
/PRIORITY	Specify an integer of 1 or higher to indicate the priority of the rule. The smaller the value the higher the priority.
/IP	Using the format: "IP Address/Mask", specify the range of client IPv6 addresses. Specify the IPv6 address by separating the hexadecimal values using colons such as "2001:200:0:1::". For the mask, either specify hexadecimal values separated by colons such as "ffff:ffff:ffff:ffff::", or you can specify the bit length from the header using a decimal value such as "64". To specify a single IPv6 host, specify the mask as "128" or "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff".